Technical Assistance Consultants' Final Report

FINAL REPORT

Project Number: TA6618
Date:8 **February** 2023

Kyrgyz Republic: Enabling a conducive environment for e-commerce

OUTPUT 1: Law and Regulation of e-Commerce

Prepared by:

- John D. Gregory–International Consultant, Canada
- Iskander Artykbaev–National Consultant, Kyrgyzstan

Beneficiary:

- Ministry of Economy and Commerce of the Kyrgyz Republic

Asian Development Bank

CONTENTS

INTRODUCTION

The era of Covid-19 has underlined what the world already knew, that the way to more effective and efficient trade, both domestic and foreign, runs through electronic communications. However, innovative business methods using such communications often encounter legal frameworks designed for paper or print media. These encounters can lead to uncertainty and sometimes to barriers to efficient transactions.

Over the past quarter century, the legal frameworks have been adjusted to accommodate and even to promote electronic transactions. Considerable efforts have been made at the international level to develop and harmonize these initiatives, notably through United Nations organizations such as UNCITRAL – the UN Commission on International Trade Law - and UNCTAD – the UN Conference on Trade and Development. Regional initiatives have come from the UN Economic and Social Commission for Asia and the Pacific – UN/ESCAP – and the Association of South-East Asian Nations – ASEAN. International financing organizations like the Asian Development Bank and the World Bank have also been involved, and more recently the World Trade Organization and the Enhanced Integrated Framework (EIF).

Regulators and traders all recognize that technology evolves more quickly than business practices, and laws that support the business practices also need to evolve to continue their usefulness. Commercial law in general tends to validate changing practices rather than controlling what practices are allowed to develop.

Where the pace of change makes specifying rules in detail difficult, there is a premium on knowledgeable flexibility. Legislation around the world governing e-commerce has become less prescriptive and more permissive over time. The challenge is to prescribe what needs to be prescribed - clear authority to do new things, precise protection of interests that need protection – and to permit individuals and businesses to transact as freely as they can within that framework.

The Asian Development Bank (ADB) has engaged us to review and report on the legal framework for e-commerce in the Kyrgyz Republic, with a view to helping ensure that its content – statutes, decrees, orders, decisions - serves the country's purposes. In particular, our

mandate is to identify legal and regulatory barriers to effective and efficient e-commerce and to develop recommendations for improvement.

All in all, the Kyrgyz Republic has done a good job keeping up with changing times. It has opted for flexibility when given the opportunity. Its most recent initiatives continue in that vein.

The present report reviews the law of the Kyrgyz Republic on electronic commerce from several aspects: electronic transactions, electronic signatures, trust services – and considers how traders and regulators have managed to operate under the law. It also considers the international legal context that importers and exporters must reckon with and the opportunities it may give for expanded operations.[1]

The report also reviews a number of particular elements of e-commerce that deserve special attention, including consumer protection, privacy and cybercrime. It concludes with recommendations for the direction of law reform in the future, notably in the light of projects that the Kyrgyz Republic has already formulated in the form of a multi-year Action Plan.[2]

This report does not include an evaluation of the technology now deployed or potentially required in order to carry out effective and efficient e-commerce in the Republic. The best laws will not produce good results if participants in the market cannot take advantage of them for lack of equipment, access to communications networks or skills to use them.[3]Likewise, lack of trust

---

1 The report takes as law some legislation enacted in late 2021, including the *Law aboutelectronic commerce,*.that may not yet be fully implemented. This Law did come into force in May 2022.

2 This report was prepared based among other things on a draft resolution of the Cabinet of Ministers of the Kyrgyz Republic "On approval of the Program for the support and development of e-commerce in the Kyrgyz Republic for 2022-2027." Online: http://koomtalkuu.gov.kg/ru/view-npa/1531/ The draft Action Plan is at the "Accompanying documents" tab in the official or the state language. The "Support program and development of e-commerce in the Kyrgyz Republic for 2022-2027" is at the main tab.The final versions of both documents were approved by the Cabinet of Ministers in December 2022 and published in January 2023. The final versions offered a few changes to the draft Action Plan and some expansion of reform details in the Support program. Action Plan:"On approval of the Program for the support and development of e-commerce in the Kyrgyz Republic for 2023-2026"Online:http://cbd.minjust.gov.kg/act/view/ru-ru/159827. "PROGRAMto support and develop e-commerce in the Kyrgyz Republic for 2023-2026", online: http://cbd.minjust.gov.kg/act/view/ru-ru/159870?cl=ru-ru. The Program in particular has a knowledgeable and subtle analysis of the issues and challenges facing the Republic in this field.

3 The CAREC Institute has recently (March 2022) published a study of e-commerce infrastructure in the member states of the CAREC Program, including the Kyrgyz Republic. Many statistics on the state of technology and popular trust are reported, along with recommendations for improvement. *E-Commerce in CAREC Countries: Infrastructure Development*, CAREC Institute and ADB, March 2022, online: https://www.adb.org/sites/default/files/publication/781526/e-commerce-carec-countries-infrastructure-development.pdf.
Readers may also be able to rely on technical analysis being conducted by the International Trade Center for the Ministry of the Economy relating to ESCAP's Framework Agreement on Facilitation of Cross-border Paperless

in intangible media, whether cultural or practical, can undermine business and consumer willingness to adopt the most efficient business methods.[4]

I. LAW OF ELECTRONIC TRANSACTIONS

Electronic communications differ from communications on paper in important ways that have challenged the application of traditional rules of law to them.[5]Understanding these differences will help explain why states, including the Kyrgyz Republic, have responded with the legislation they have and what measures are appropriate for further development.

Invisible processes. Electronic communications are created through the use and interpretation of electronic signals. This provides numerous benefits to commerce and the public at large. The main challenge in law arises from the fact that the computations used to deliver text and numeric information are invisible. Users have to trust the computers involved to do it right, and to do it the same way every time—i.e., to display on the screen or to send to the printer the same text for every party to a transaction and everyone else with an interest in it, such as auditors, regulators, and tax authorities. However, bits and bytes can degrade or be changed undetectably, leaving the resulting screen or printed text looking as perfect as the original. This is not the case with paper, where it is difficult to amend an original document without leaving a trace.

Rapid evolution of the technology. What one understands about the operations and risks of technology today may not be true tomorrow.

Legal uncertainties and doubts. Any user of a computer connected to a communications system may have cause to worry about intrusions into the computer for malicious or even criminal purposes. Consumers also wonder whether what they might buy online will be what is delivered to them, as well as whether they will have any remedy against a remote online merchant if the product that arrives is bad. The question for the merchants may be whether their remote online customers will pay them.

Trade in Asia and the Pacific. That work involves a review of the Kyrgyz Republic' technical readiness for such trade.UN International Trade Centre, Ready4Trade Central Asia, *Report on the assessment of the level of readiness of the Kyrgyz Republic for cross-border paperless trade*, DRAFT English text, 2022

[4] ADB and United Nations (UN) Economic and Social Commission for Asia and the Pacific (ESCAP). Manila, 2018. *Embracing the E-Commerce Revolution in Asia and the Pacific*. https://www.adb.org/sites/default/files/publication/430401/embracing-e-commerce-revolution.pdf .

[5] World Economic Forum, *Making Deals in Cyberspace: What's the Problem?*, White Paper, October 2017. Online: https://www.weforum.org/whitepapers/making-deals-in-cyberspace-what-s-the-problem

Concern about misuse of personal data. It is easy for operators of electronic communications systems to “harvest” the data about individuals engaged in such communications. Not everyone trusts the legal rules set up to keep the collection, use and disclosure of personal information within acceptable bounds.

Different approaches and rules in different places. Electronic information crosses borders easily, but the rules for resolving its legal status may differ from one place to the next, and arranging for recognition of the effect of foreign rules has been difficult.

The result of these and many other uncertainties has been unwillingness by some to trust electronic communications and e-commerce and a belief that the laws that apply to paper communications are inadequate to ensure confidence in the integrity of the products of electronic communications. When electronic communications first appeared in commerce, the existing laws protecting the integrity of paper documents did not fit them well or were difficult to apply.

In the past decades, a broad international consensus has developed on how to manage the transition of legal frameworks to electronic communications. In addition, e-commerce transactions have expanded all over the world even in the absence of supporting legislation. The question here is how to remove the remaining barriers—those governing electronic transactions—and channel e-commerce in a way that encourages its growth in a safe, sustainable manner.

This report discusses the international best practices – legislative and other – and indicates what may still be missing to optimize the Kyrgyz Republic’s ability to manage e-communications in its legal system.

Moreover, private technology will continue to offer new methods of doing e-commerce more securely. The law should leave room for the use of devices, codes, and platforms that are yet to be developed but that could avoid the need for some state regulation or administrative supervision.

Continuing dialogue between the private and public sector, including development partners, is important. For example, the United Nations Conference for Trade and Development (UNCTAD) has launched the Business for E-Trade Development platform, comprising a private sector advisory group, to optimize and support public policies for e-commerce development worldwide.[6] UN/ESCAP's technical and legal advisory groups can play a similar role.

International best practices
Best practices in this area derive from the UNCITRAL Model Law on Electronic Commerce.[7] The Model Law says that information shall not be denied legal effect, validity or enforcement solely on the grounds that it is in the form of a data message (i.e., in electronic form).

A. Electronic Transactions

In 1996, UNCITRAL adopted the Model Law on Electronic Commerce (MLEC), which has been enacted in more than 80 countries and remains the best template for e-commerce legal reforms.[8] Because it is a model law rather than a convention, the MLEC can be applied by any legal system and adapted to fit into any legislative regime. The MLEC deals principally with form requirements, rather than with rules of substantive law. The MLEC also leaves a good deal of autonomy to transacting parties to decide how to satisfy its rules.

Electronic documents: The main challenge to the validity and use of e-documents has often been legal requirements that certain documents be in writing. UNCITRAL's MLEC provides that electronic documents can satisfy that requirement when their information is accessible so as to be usable for subsequent reference. Another barrier to the use of e-documents is the common requirement for the original versions of documents to be produced for legal purposes. The MLEC provides a method of analyzing information in electronic form to decide if it is a functional

6 Online: https://unctad.org/system/files/non-official-document/dtl_eWeek2017p15_DanielCrosby_en.pdf
7 UNCITRAL, Model Law on Electronic Commerce, 1996, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
8 Footnote 7.

equivalent of a paper original, i.e., can the electronic version achieve the policy goal (the function) that lies behind the traditional legal rule? The key element for a functional equivalent to an original, according to UNCITRAL, is whether the information can be shown to have retained its integrity from the time it was created until the time of analysis.

Sales

The basic activity of electronic commerce is the commercial transaction, often a sale from one party to another. Most of the substantive law of sales is "media neutral" – it can apply to material or online transactions equally. As a consequence, questions of capacity of parties to contract (e.g. age, sobriety) or the mental element in a contract (e.g. consent, knowledge of what is being contracted for) are not different for electronic commerce than for transactions documented on paper.

General sales law is governed by the *Civil Code of the Kyrgyz Republic*.[9] The *Civil Code* does not require transactions to be in writing – they may be oral. If they are put in writing, the written document does not need to be signed in order to be legally valid, though most parties sign them as a matter of prudence: a signature makes it easier to demonstrate attribution (origin) and consent if there is a dispute later.

This section of the Report considers the nature of electronic transactions and of electronic signatures, in the Kyrgyz context.

The *Law about Electronic commerce* of 2021[10]defines an electronic transaction as a civil legal transaction between participants in electronic commerce through information and communication technologies, concluded in accordance with the requirements of this Law and the civil legislation of the Kyrgyz Republic (i.e. the *Civil Code* mentioned above.)[11]

The Kyrgyz equivalent for documents is supported by the statute's declaration as a principle of electronic commerce "recognition of the legal force of electronic documents, regardless of the method of their conclusion and signing."[12]

---

9 The *Civil Code of the Kyrgyz Republic* is online: https://cis-legislation.com/document.fwx?rgn=51 (part 1)

10 *Law about electronic commerce*, 2021 No. 154,online: https://cis-legislation.com/document.fwx?rgn=136937. The full text in Russian is available for free at http://cbd.minjust.gov.kg/act/view/ru-ru/112333.

11 Footnote 10, article 3(2) 14).

12 Footnote 10.

Two of the other "principles of electronic commerce" set out in article 4 of the Law are "ensuring the legal rights and obligations of participants in economic activity" and "legality of electronic transactions."

As a result, the legal effectiveness of electronic transactions is secure in the Kyrgyz Republic for "the sale, purchase and exchange of goods and/or works and/or services, including exclusive rights to intellectual property."[13]

As in most countries, however, the Law does not apply to all possible transactions. Notably, it excludes:

- transactions subject to notarization and/or state registration,
- goods, works and services in respect of which restrictions have been introduced to ensure safety, protection of human life and health, protection of nature and cultural values;
- procedures for public procurement.[14]

The Law also provides that electronic messages may be electronic documents, if they have legal consequences for any party. The only practical difference between an e-message and an e-document is that the former moves at some point from sender to recipient to storage, while the latter is less mobile (though it may be attached to a message.)An e-document may be machine-readable or readable by humans, or both. Electronic documents in either form have the same legal force and are an integral part of the electronic contract that usually constitutes the electronic transaction.[15]

1. Electronic trading platforms

The Law about e-commerce contemplates substantial numbers of transactions being conducted through "trading platforms", defined as "a set of software and hardware that ensures the sale of goods and/or works and/or services via the Internet." The trading platform provides a forum for

[13] Footnote 10, article 1(2).
[14] Footnote 10, article 1(3). There is no express exclusion of electronic transferable records, those that carry title to goods with possession of the record itself, such as a bill of lading. It is also not clear that such records would be satisfactorily covered by the current text of the Law. The international standard for such records is the UNCITRAL Model Law on Transferable Electronic Records, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
[15] Footnote 10, article 13.

sellers of goods to put their wares on the market, presumably in the expectation that sellers do not have the skills or equipment themselves to address the Internet directly. Benefits of platforms to transacting parties include pooling certain services (payment, delivery, etc.) and getting visibility due to the significant overall offer of products and services (as opposed to a merchant's individual website, or even a webpage on social media).

The obligations of trading platform operators in article 6 include making the seller's goods and services available; keeping separate the seller's and the platform operator's interests; creating a policy for users of the platform "ensuring the quality of goods and services" and "protecting the interests of consumers and information of a personal and commercial nature;" providing the ability to search the platform for goods or services sorted by price, sales and other criteria, and assisting participants in an electronic transaction in protecting their rights and interests.

The E-Commerce Association of the Kyrgyz Republic has proposed that the law should have added to it "the rights of sellers, operators of a trade platform," and "redistribute and harmonize the rights and obligations of sellers, trading platform operators and consumers." It has not indicated why the contents and balance of those rights and obligations in the current statute is unsatisfactory.[16]

It is worth noting here that the Eurasian Economic Union (EAEU) of which the Kyrgyz Republic is a member has been developing standard policies for its member states on how to carry out e-commerce through trading platforms.[17] The provisions here should be aligned with the EAEU policies once the latter are formally in place.[18]

[16] Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 1.
[17] See the discussion about international connections and influences, below, section III, text at footnote74
[18] The EAEU is discussed below at section III.C.b. At present there are no final rules for e-commerce platforms.

B. Electronic Signatures

International best practices
The international legal framework for electronic signatures starts with the UNCITRAL Model Law on Electronic Signatures (MLES),[19] as updated by the U.N. Electronic Communications Convention (ECC)[20] in 2005. These documents provide that where the law requires a signature, an electronic signature will satisfy the requirement if the electronic method of signing reliably identifies the signatory and indicates its intention with respect to the signed document.
Both the MLEC and the ECC provide rules on what may make an e-signature reliable. The signing device must be associated only with the signatory; the device must be in the sole control of the signatory, and any change to the signature (and sometimes the document) after signing must be detectable. (MLES 9.6))[21]
At the higher end of the reliability scale are digital signatures, described below.
There can be tension between the need for reliability and the need for manageability. Different social and business purposes may demand different levels of trust. (See the discussion of trust services, below.)

The Kyrgyz Republic has in the past decade taken significant steps to relax the demands on electronic signatures. Its legislation provides considerable flexibility in the use of what it calls "simple" electronic signatures, though arrangements are also available for certificated digital signatures in appropriate cases, as prescribed by law.

While contracting parties do not need to sign their written or electronic documents, it remains prudent to do so. Once one signs an electronic document, the signature is governed by the *Law*

[19] UNCITRAL Model Law on Electronic Signatures, 2001, (MLES), online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.
[20] UN Convention on the Use of Electronic Communications in International Contracts, 2005, online: https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications.
[21] The MLES says that where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, then any alteration to that information needs to be detectable too. Article 6(3)(d). Not all legal systems expect a signature to support the integrity of the signed information.

on electronic signature.[22]As noted above, the legal force of electronic documents is recognized regardless of the method of their conclusion and signing.

An electronic signature is defined as "information in electronic form that is attached to other information in electronic form and (or) logically connected with it and which is used to determine the person on whose behalf the information is signed."[23] This is close to the description of the functional equivalent of a signature in the UNCITRAL Model Law on Electronic Signatures[24] (and the definition of electronic signature in the United Nations Electronic Communications Convention)[25], but without the need for appropriate reliability.[26]

Parties are free to use any type of electronic signature, if the law does not provide otherwise.[27]The statute provides for three kinds of electronic signature: simple, unqualified enhanced and qualified enhanced.[28]

- The simple e-signature is "an electronic signature, the signature key of which coincides with the electronic signature itself (codes, passwords and other identifiers)."[29] It seems likely that this definition would apply to a name typed at the bottom of an email – an "other identifier".
- An unqualified (enhanced) e-signature is one that meets conditions very like those that the UNCITRAL Model Law on Electronic Signatures presumes make an e-signature reliable:[30]the signature creation data are under control of signer, the signature allows unique identification of the signer, the signature allows detection of changes made to the document after its signing. In addition, such a signature is created by cryptographic key.[31]
- A qualified (enhanced) e-signature has the characteristics of the unqualified one, plus its signing key is indicated in a qualified certificate,[32] which is one issued by an accredited certification centre.[33] See the next subsection of this report on Trust Services.

---

22 *Law about electronic signature* (2017), online: http://cis-legislation.com/document.fwx?rgn=99019 article 1(1).
23 Footnote 22, article 2(1).
24 Footnote 19.
25 Footnote 20.
26 It is a good thing to have omitted the "reliability" test. See J.D. Gregory, "Must E-Signatures be Reliable?" online: https://journals.sas.ac.uk/deeslr/article/view/2024/1961.
27 Footnote 22, article 4(1).
28 Footnote 22, article5(1).
29 Footnote 22, article 5(2).
30 UNCITRAL Model Law on Electronic Signatures, footnote 19, article 6(3).
31 Footnote 22, article 5(3).
32 Footnote 22, article 5(4).
33 Footnote 22, article 1(3).

The equality of legal status among the classes of e-signature (in the absence of specific contrary legislation) is shown by the fourth "principle" of using an electronic signature: "the inadmissibility of recognizing an electronic signature and (or) an electronic document signed by it as null and void only on the grounds that the signature in the electronic document is not a handwritten signature."[34]

Both a simple e-signature and an unqualified e-signature can have the effect of a handwritten signature, "in cases established by regulatory legal acts or by agreement of electronic interaction participants," unless the use of electronic means is prohibited by law.[35]So far as we can tell, there are no "cases established by regulatory legal acts" – it is up to transacting parties to decide on the level of signature they want.

In short, parties to a transaction may agree to use simple signatures to meet legal signing requirements and presumably may agree on the degree of reliability, including the type of technology, that they will accept for this purpose.[36]However, simple signatures may not be used to sign documents containing state secrets.[37]

If one wants to use an unqualified e-signature as the equivalent of a handwritten signature, one must "provide for the procedure for verifying electronic signature."[38] Since the unqualified signature has defined characteristics, one must be prepared to show that those characteristics are present in one's signature. An unqualified signature is supported by a certificate issued by a certification center (unless its characteristics can be established without a certificate.[39]) See the discussion of Trust Services in the next subsection of this report.

A qualified e-signature is the equivalent of a handwritten signature unless the law prohibits using e-documents for the purpose.[40]Again, we are unable to find any such prohibition, though the law is in evolution. In other words, an unqualified e-signature is equivalent to a handwritten

[34] Footnote 22, article 4(4).
[35] Footnote 22, article 6(2). (The translation of the provision says "unless laws or other regulatory legal acts do NOT prohibit the compilation of such a document in electronic form." The "not" appears out of place.)
[36] See footnote 22, article 9(3) for more content of an agreement to use a simple signature. The technology neutrality of the e-signature requirements is also affirmed by the second principle of using an electronic signature, in article 4(2), subject to displacement by a specific provision or agreement of the parties, according to article 4(1).
[37] Footnote 22, article 9(5).
[38] Footnote 22, article 6(2).
[39] Footnote 22, article 5(5).
[40] Footnote 22, article 6(1).

one where the law says so ("established by regulatory legal acts") or the parties agree. A qualified e-signature is equivalent unless the law prevents that equivalence.

An unqualified or qualified (but not a simple) e-signature may be the equivalent of a seal in a document on paper, unless a specific law requires something more.[41] Seals are not mandatory in Kyrgyz law, but parties may agree to use them on their transactional documents.

One may conclude that the Kyrgyz law on electronic signatures conforms well to international standards. It offers a good deal of flexibility to transacting parties, and to citizens who want to communicate with the government or public agencies. That topic (communication with government) is discussed in more detail below.

Potential law reform in this area is discussed in section IV below, "Proposed E-Transaction Laws".

The use of electronic documents and the classes of e-signatures for state bodies is spelled out in the *Law about e-governance*.[42]

1. Trust services

Trust services support the authentication of electronic messages. Trust service providers are often issuers of the data (codes, encryption keys) used to create electronic signatures, and even more often the issuers of certificates that link the signature data embedded in an electronic signature with the legal person or entity who used the data to sign something. A person's e-signature may be incomprehensible code, and the certificate interprets the code to say 'this signature belongs to X'.

The trust services in the Kyrgyz Republic are called certification centers – issuers of the certificates linking signing data to legal persons.[43]

The 'trust' in trust services is the trust generated in the person asked to rely on the e-signature that the e-signature is actually from the person it says it is from.

---

41 Footnote 22, article 6(3).

42 *Law about e-governance*(2017), No. 127, amended 2020 No. 94, article 16, online: http://cis-legislation.com/document.fwx?rgn=99015. (The CIS legislative database titles this "Law about electronic control," but retranslating it from the Russian with Google Translate produces the more helpful "e-governance" phrase.)

43 Footnote 10, article 2(6)('signature verification key') and (7)('certification center … engaged in the creation and issuance of signature verification key certificates').

Some trust services will in practice be more trustworthy than others. That is why the electronic signatures law contains considerable detail about the establishment of certification centers, the difference between accredited and non-accredited centers (with only the accredited ones allowed to certify a qualified e-signature), their liability to other users, the contents of certificates, the duties of the parties to an e-signature of different classes, and so on.

A Decision of the Government sets out more detailed rules for the accreditation of certification centers.[44] They are much like provisions on the same topic in other countries' statutes, and to a degree derive from similar provisions in the UNCITRAL Model Law on Electronic Signatures concerning the reliability of certification service providers.[45]

Most recently, UNCITRAL's Working Group on Electronic Commerce has developed a Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services[46] that was adopted in the plenary session of UNCITRAL in June 2022. Its statements of the duties of identity managers (those who identify commercial participants and confirm their attributes) and trust service providers (articles 6 and 10 of the Model Law) may become the international best practices, given the success of UNCITRAL's formulation of such rules in the past. It will make sense for the Kyrgyz Republic to consider whether its laws are consistent in principle with this new Model Law. It will be particularly useful in transactions involving the European Union, whose current laws resemble the new UNCITRAL Model Law. Current Kyrgyz laws are not far from doing so already; there should be few if any policy issues in the implementation in due course.

It can be noted here that the Eurasian Economic Union (EAEU), of which the Kyrgyz Republic is a member, has been developing its "transboundary trust environment" for several years.[47]It is

---

[44] Decision of the Government of the Kyrgyz Republic, December 31, 2019, No. 742, amended December 17, 2021, No. 310: online:https://cis-legislation.com/document.fwx?rgn=121880.

[45]Footnote 19, article 10.

[46] The draft Model Law is online as document A/CN.9/1112, 21 February 2022: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf.

[47] DECLARATION of 6 December 2018 on further development of integration processes within the Eurasian Economic Union, online: https://docs.eaeunion.org/docs/en-us/01422031/ms_10122018. (This is in Russian despite URL). The program includes:
Article 2 (part): creating the common digital business space based on harmonization of approaches and compatibility of technologies, in particular, developing a notion of a cross-border space of trust and mutual recognition of legal importance of digital processes and services.
The commentary on the draft UNCITRAL Model Law on Identity Management referred to in Footnote 45 says (at paragraph 51) that the system rules of an identity management arrangement can be thought of as a "trust

building its system by starting with government documents shared between governments that trust each other, yet the work is slow. In short, even with similar and closely cooperating states with community institutions, the task is difficult. More information on the EAEU appears below, in the section on international arrangements affecting e-commerce.[48]

2. Digital signatures

The 'enhanced' e-signatures in the Kyrgyz law, whether qualified or unqualified, are in technical language 'digital signatures'. A digital signature is, as article 5(3) of the *Law about electronic signatures* puts it, "obtained as a result of cryptographic transformation of information using the signature key". The cryptography involved is known as 'dual key' or 'public key' cryptography. The two mathematical keys are generated together (usually by a certification center, as in the Kyrgyz case) and function so that what is encrypted with one key (the "private key") can be decrypted only by the other (the "public key"). If a party known (because certified) to have one of the key pair signs something with that key, then someone decrypting the signature with the other key can be confident that it was signed by the party named in the certificate.[49]

This system depends on the security of the signing device (e.g. computer, phone, tablet) containing the private (signing) key, so that nobody other than the certified party can sign anything with it. For that reason, the laws on the topic, including sub-article 5(3) 4) here, require that any compromise of the security of the signing device or of the signing data in the device must be reported and almost certainly invalidates future signatures using that data (and to an extent past signatures as well, if they have not been relied on before the compromise is discovered.)

There are other technical requirements for the usual use of digital signatures that are beyond the scope of this article. (The whole system of rules and practices is known as a Public Key Infrastructure, or PKI.[50]) Those requirements are very much in the mainstream of how digital signatures are governed around the world.[51] While the UNCITRAL Model Law on Electronic

framework". The EAEU's work clearly overlaps to some extent with UNCITRAL's or serves as an example of what UNCITRAL is promoting.

48 See below, text at note 96.

49 Dual keys may be used in the opposite direction as well. Someone may sign a document with the public key, knowing reliably that only the holder of the private key will be able to read it.

50 The technical operations of the Kyrgyz Republic's PKI are described at the Infocom (certification center's) website: https://infocom.kg/ru/pki

51 Cybersecurity and Infrastructure Security Agency (USA), "How digital signatures work", updated 2020, online: https://www.cisa.gov/uscert/ncas/tips/ST04-018. A more thorough review of digital signatures in the context of global laws on signatures and authentication was published in 2007 by UNCITRAL, "Promoting confidence in

Signatures that is a model for the Kyrgyz legislation is phrased in technology-neutral language, i.e., it does not expressly require any particular technology to operate, in practice it is usually taken to describe digital signatures using public-key cryptography.

3. Foreign signatures and certificates

The Kyrgyz statute reflects the Model Law on Electronic Signatures in its rules on recognition of foreign signatures. There is to be no discrimination against an e-signature or e-document solely because the signature certificate "is issued in accordance with the law of a foreign state."[52] An e-signature created under foreign law standards is recognized as the equivalent to a Kyrgyz signature of the same sort.[53] While this does not expressly focus on the similarity of level of reliability of the foreign e-signature, that seems likely to be the focus of any inquiry.

II. ELECTRONIC TRANSACTIONS IN PRACTICE

As noted, the laws of the Kyrgyz Republic have been becoming more accommodating to electronic commerce over the past decade or more. The text of legislation is not always reflected in commercial practice, however, for one reason or another. It may be that business people are not aware of their opportunities to go electronic, or they lack the technical skills to do so, or they lack the computer equipment. The same may be true of their potential trading partners, at home or abroad. Perhaps the permissions in the legislation are not clear enough to prompt a change of behavior.

To estimate the gap, if any, between the legislative theory and the business practice, our team (notably Mr Iskander Artykbaev) interviewed a number of people in different sectors of the trading universe in the Republic. This section notes his findings and our observations on them.

A. The private sector

There is some evidence that the challenges to doing business electronically do not arise principally from deficiencies in the law but from cultural and technological barriers.

On the cultural side, the vast majority of buyers prefer to rely on ink signatures on paper, even though e-signatures are permitted by law. To some extent, business people may be waiting to see if some of the "other" rules referred to in the *Law about electronic commerce* are enacted –

---

electronic commerce: legal issues on international use of electronic authentication and signature methods", online https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698_ebook.pdf. Digital signatures are discussed at pages 17 to 27.

[52] *Law about Electronic Signatures*, footnote 22,article 7(2).

[53] Footnote 22, article 7(1).

limits or permissions that in strict logic may not be needed for the general permission of the statute to be effective. One understands caution on such matters, however, especially where there is little tradition of trust in e-communications generally. However, at time of writing (October 2022), the government had not announced any plans for implementing regulations for this statute.

There is also a cultural preference to pay for purchases in cash, rather than paying electronically (notably through credit cards). Though the people of the Kyrgyz Republic have about 3 million credit cards (2020 figures), a large proportion of card transactions were cash withdrawals. In 2015, 90% of card transactions were merely withdrawals from bank accounts. By 2020, half the transactions in Bishkek were e-commerce transactions, but the proportion in smaller areas was much more in favour of not-very-commercial dealings with cards.[54]This suggests a lack of integration of payment systems and online stores.

On the technology side, there is also a lack of broadband Internet access in the country – and it is much harder to shop online with dial-up connections. Further, the country is not heavily urbanized, which means that broadband will spread slowly. And even when connected, there is widespread distrust of the fate of one's personal information through online shopping. That may be a defect in the privacy legislation mentioned later in this report, or at least in how it is perceived by the public.

The cost of delivery of packages bought online is high, even in the capital, another disincentive to buy through that medium.

[54] Support Program document, Footnote 2,mentions the newest statistics at page 3. The present discussion is echoed below in Section V:F, electronic payments.

B. The public sector

International best practices
The United Nations Centre for Trade Facilitation (CEFACT), part of the Economic Commission for Europe, has two main guides for countries developing a single window:

1. Recommendation 33: Establishing a single window [55]
2. Recommendation 35: Establishing a legal framework for a single window. [56]

The ESCAP Framework Agreement on Cross-Border Paperless Trade in Asia and the Pacific also encourages member states to establish a single window to facilitate and economize on the technical communications it deals with.
The WTO Trade Facilitation Agreement (TFA) likewise encourages member states to establish a single window for this purpose. [57]

1. Single window

One of the main activities that facilitates cross-border paperless trade is the creation of a "single window", which is a central clearing-house or communications hub for documents requiring regulatory approval, for imports or for exports. The importer, or carrier on behalf of the importer, or the exporter, can file (lodge) all documents for the destination country in one place, with one office, or – electronically – one electronic address. From there, the documents are automatically sent to the appropriate authorities for review. When the regulator has made its decision, that decision is communicated back to the importer or exporter through the same 'window' of communications. The E-Commerce Association of the Kyrgyz Republic has advocated for a

[55] Online: https://unece.org/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf
[56] Online: https://digitallibrary.un.org/record/668437?ln=en
[57] WTO Trade Facilitation Agreement article 10(4), online: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/940.pdf&Open=True. Article 10(4.1): "Members shall endeavour to establish or maintain a single window, enabling traders to submit documentation and/or data requirements for importation, exportation, or transit of goods through a single entry point to the participating authorities or agencies."

single window system, described as “electronic interaction between the state bodies and participants in external economic activity.”[58]

In the Kyrgyz Republic, the Ministry of Economy and Trade has responsibility for developing a national single window. Normally the lead ministry builds a team of representatives from the main regulatory authorities within government, those that are called on to inspect or consider goods and services proposed for import (or export), along with private sector interests. This coordinating committee would ensure that everyone’s capacities and interests are considered in building a system.

Normally as well, a statute is developed to ensure that the legal authority to participate and to collaborate in the single window system is clear. The contents of the statute and other inter ministerial agreements in support may be inspired by the CEFACT Guide to legal issues, noted above. In addition, UN/ESCAP has published a guide to building capacity to create a single window operation.[59]

The multi-year Action Plan for e-commerce in the Kyrgyz Republic[60]speaks of ensuring that government departments can communicate with each other electronically, to help support such a common Endeavour. (The *Law about electronic governance* contemplates a system of interdepartmental electronic interaction – in article 22 – that may support such communications.)[61]

The Action Plan wants to bring into the communications system as well “participants of foreign economic activity”, which presumably means both foreigners and nationals of the Kyrgyz Republic who are so engaged. One would want to include foreigners’ opinions in building a national single window.

The Action Plan schedules this item for the third quarter of 2026.

---

58 Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 11.

59 *The UNNExT Electronic Single Window Legal Issues: A Capacity-Building Guide*, online: https://www.unescap.org/resources/electronic-single-window-legal-issues-capacity-building-guide (available also in Russian). UN/CEFACT issued Recs. 33 and 35 on the topic.

60 Footnote 2. See item 8 on the present matter, which has been reworked into support for a Single Window or “One Stop Shop” for documents.

61 *Law about electronic governance*, footnote 42.

Our recommendation is in favour of legislation for the basic principles and permissions of a single window, though it may be supplemented by a network of contracts by which participants bind themselves to performance standards that may be enforceable by civil liability.

2. Electronic portal of public services

The Ministry of Digital Development is building an electronic portal by which Kyrgyz citizens and residents may communicate and transact with all levels of government. The portal, https//portal.tunduk.kg, at time of writing has over 900 services offered online.[62]It seems like a very popular service, perhaps supported in its popularity by being a prime source of certificates of vaccination against the Covid virus.[63]

The Ministry[64] is responsible for the *Law on Electronic Governance*.[65] It has taken over the functions of the Council for the Transition to Electronic Governance mentioned in that Law.[66]

3. Unified identification system

As noted earlier, the *Law about Electronic Signature* contemplates special rules for types of e-signatures used by "executive authorities and local governments".[67] In addition, the *Law on E-governance*[68] contains an entire regime for electronic dealings between state and residents in the Republic – the portal just described.

The *Law on e-governance* has an interesting set of provisions on authorizing citizens' access to information in public information systems like the portal. It relies on identifying citizens through qualified certificates of keys for verifying electronic signatures (i.e. public keys) and confirming their identity in the state records.[69] This allows for more efficient communication among citizens and different departments of government.

More unusual is a provision that allows any person who applies for state and municipal services to be issued an "activation code and a key of simple electronic signatures" for registration in a

---

62 A description of the portal in more detail is online: https://infocom.kg/ru/news/499-dlia-ghrazhdan-kyrghyzstana-do-31-diekabria-2021-dieistvuiet-vozmozhnost-biesplatno-poluchit-oblachnuiu-eliektronnuiu-tsifrovuiu-podpis/

63 See the Kaktus Media story on the portal and digital signatures cited in footnote 71 below for the main uses being made of the portal.

64 The Ministry's main website is: https://digital.gov.kg/ in Russian and English.

65 Footnote 42.

66 Meeting between Ministry and Iskander Artykbaev on January 25 2022.Those paragraphs of this Law, which relate to the electronic digital signature, have lost their relevance to a certain extent.

67 Footnote 42, article 3(3).

68 Footnote 42.

69 Footnote 42 article 23.

unified information system. Currently, the state enterprise known as Infocom has the responsibility for assigning a digital cloud electronic signature to everyone. The resulting electronic signature allows citizens to use certain public services.

Such keys are made available for free to any adult citizen for the asking. The Ministry of Digital Development has said that the keys may be used not only for dealing with the government but also in citizen-to-citizen transactions.[70]Applicants for such e-signature keys must use their passports to authenticate themselves on enrolling in the national Public Key Infrastructure and acquiring digital signing data.[71]The keys are to be embedded in the electronic national identity card and serve as an electronic digital signature. The signatures for free distribution remain "simple" e-signatures within the meaning of the *Law about electronic signatures*. Enhanced e-signatures still require an application to the certification center, and payment.[72]

This initiative could lead to much more secure yet economical communications among citizens (including their businesses) using a trusted government resource. Its impact on the adoption of e-commerce among citizens of the Republic remains to be seen, but it has the potential to be helpful.

C. The Customs Authority

The State Customs Service of the Kyrgyz Republic has been dealing with e-commerce under the rules of the *Customs Code* of the EAEU, working on a system to accommodate the exclusions provided in that Code measured by size and value of the packages. It has also been calculating the volume and value of shipments originating in electronic commerce, but no definitive statistics are yet available.

In November 2021, the Republic joined the Revised Kyoto Convention on the Simplification and Harmonization of Customs Procedures. The main feature of the Convention is to have customs authorities apply a risk-based screen on imports. Shippers with good records and shipments of lower value may have their screening at the border expedited or done in bulk, to save time with

---

[70] Conversation between Ministry and IskanderArtykbaev, January 2022.

[71] A description of the system appears in Kaktus Media, "Electronic signature in Kyrgyzstan is now free. And here's how to get it", 31 March 2022, online: https://kaktus.media/doc/457366_elektronnaia_podpis_v_kyrgyzstane_teper_besplatnaia._i_vot_kak_ee_polychit.html (automatically translated into English by the Chrome browser.)

[72] The operation of the identification card with embedded digital electronic signature is described in this 2017 document: https://grs.gov.kg/ru/eid/digital_signature/ It largely contemplates a citizen-to-state use of such signatures and does not mention citizen-to-citizen uses or, of course, the general 2021/22 distribution.

an acceptably low probability of dishonesty or mistake that would cause loss of revenue. (It is possible that they will become 'authorized economic operators' in the world of e-customs. Participants in trade in any capacity who achieve that status benefit from streamlined procedures and built-in trust that facilitates their activities.)[73]The novelty of the task means that the Customs Service is in its early days of calculating and applying this type of analysis. It clearly represents the global best practice.

Some countries' customs authorities have difficulty handling the volume of shipments that e-commerce can create, especially high volumes of relatively low-value packages. The ability to do so does not depend on legislative or regulatory reform at this point, but on administration and technology. Consultation and harmonization with neighboring states will be helpful.

One of the most important documents that accompanies goods imported or exported is a certificate of origin, attesting to the country where the goods, or a substantial part of their value, originated. This information allows Customs to know how to handle the goods and what level of duties to impose, if any. Customs processing can become much faster if such certificates are in digital form (and standard form). Private initiative will be important, since manufacturers are best placed to know the origin of the goods and their components. The Action Plan mentions the Chamber of Commerce and Industry as a participant in developing the appropriate certificate(s) and schedules electronic certificates of origin for the 4th quarter of 2024. Cooperation will be needed with trading partners to ensure the acceptability of the e-certificates abroad, and presumably the acceptability of foreign e-certificates in the Kyrgyz Republic. A regional standard for them is conceivable, probably through the EAEU.

D. Regulators of import or export businesses

Importers and exporters are subject to many regulations, depending on the goods (or more rarely services) that they bring or send across the border. The source of the regulations may be almost any government department. It is usually in the interests of efficiency that any communication between importers and exporters, on the one hand, and regulatory agencies, on the other, should be done electronically.

[73] The AEO system and its place in the broader world customs picture are explained in the WCO's "AEO Validator Guide", online: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/aeo-validator-guide.pdf?la=en.

Making these communications electronic requires standardized formatsfor information, i.e. forms, to be converted to electronic form. Ideally the forms would be machine-readable, to save on repeated data entry with its delay and its risk of error.

This section mentions briefly some of the principal regulatory jurisdictions in the Kyrgyz Republic and discusses the prospects for their carrying out their activities by electronic means. This discussion is related to the single window issue, since many of the 'regulators' would review import or export applications coming to it through the single window. As a result, the actual legal authority for using e-documents is mentioned in the following section of this report, on international instruments.

1. Ministry of Agriculture
    a. Sanitary and Phytosanitary Certificates (SPS)

Electronic certificates are allowed under conventions mentioned in the next section.

    b. Trade in endangered species

Electronic certificates (of inspection, of origin) are allowed under conventions mentioned in the next section.

2. Product safety standards are important to comply with consumer protection rules that are increasingly prominent in international trade agreements (mentioned in the following section.)

3. Other foreseeable areas of regulatory interest for goods and services crossing the border in either direction

III. INTERNATIONAL FRAMEWORK: OBLIGATIONS AND POSSIBILITIES

Like other countries, the Kyrgyz Republic is party to a number of international commercial or trade agreements, and it could become party to others. Many of these either expressly authorize the use of e-communications or are expressed in media-neutral terms that would allow e-communications if those acting under the agreements (businesses or governments) chose to use them.

If the local laws tended to restrict e-communications, sometimes transacting parties could rely on the international agreements for their authority to go paperless. This is true in part because Kyrgyz law often says that in the event of conflict between a national law and a treaty obligation, the treaty obligation prevails. It is also true in part simply because the international instrument may have a wider scope than the national one and leave more room for innovative practice across the border.

This is not so much a factor of concern today with the Kyrgyz Republic, whose policies favor such communications where possible, but international instruments may still fill gaps in policy permissions or offer flexibility in approaches to the use of ICTs.

In addition, some agreements are expressly about e-communications.
Moreover, one finds recognized international standards that can be used as the basis for e-communications technology, without the country having to join any body or agree legally to refer to the standards.[74]

A. Trade agreements that affect e-commerce

International free trade agreements have in the past decade begun including provisions to harmonize the legal regimes governing e-commerce in the participating countries. This has not been incidental or merely for facilitation; instead, these agreements explicitly promote reforms to commercial law to frame the legal effect of e-commerce. The World Economic Forum has reported that over half of the trade agreements currently in operation contain an e-commerce chapter which set out commitments to the facilitation of e-commerce.[75]

In some cases, the provisions aim only to bring the parties to a uniform level in their implementation of global standards. Such standards include the UN Commission on International Trade Law (UNCITRAL) model laws.[76] The provisions aim in other cases to compel parties to the trade agreements to adopt particular positions on controversial policies,

[74] Much of the explanatory text in this section is taken or slightly adapted from the principal author's report on CAREC E-commerce legislation published in 2021 by the ADB.*E-Commerce in CAREC Countries: Laws and Policies.* Online: https://www.adb.org/publications/e-commerce-carec-laws-policies.

[75] National Center for Asia-Pacific Cooperation, Working Group on E-Signatures, *Advancing Digital Transactions in APEC: Enhancing E-Signatures and digital Signatures,*March 2022, p 15. Online: https://ncapec.org/library/AdvancingDigitalTransactionsinAPECEnhancingE-SignaturesandDigitalSignatures.pdf. An alternative and perhaps more accurate formulation: more than half of WTO members have signed at least one [Regional Trade Agreement] that contain a standalone e-commerce provision. A. Darsinouei and R.Kakaub, "Understanding E-Commerce Issues in Trade Agreements", Geneva: CUTS International, 2017, 11. Online: https://www.cuts-geneva.org/pdf/STUDY%20-%20E-Commerce%20Towards%20MC11.pdf.

[76] Model Law on Electronic Commerce, Footnote 7, and Model Law on Electronic Signatures, Footnote 19.

such as a requirement that businesses should or should not locate data processing facilities in the country from which the data (particularly personal data) originate.

The phenomenon of pursuing paperless trade facilitation in recent international trade agreements was examined in 2017 by the Asian Development Bank (ADB) Institute focusing on electronic trade facilitation rather than on legal reforms that apply to private transactions.[77] Other papers, including from the World Trade Organization, note several agreements with e-commerce provisions.[78]
Given differing legal and cultural traditions of the parties involved, trade obligations are often at a high level or are aspirational, making it difficult to use them to support commercially effective legislation or resolve practical implementation issues. These provisions state goals that the parties hope to somehow achieve one day but do not help to arrive at them.

Nevertheless, amid the heightened importance of digital trade and reinforced by the pandemic, trade agreements have emerged to the forefront of rule-making on digital trade issues. Notably, the Australia-Singapore Digital Economic Partnership Agreement,[79] the Digital Economy Partnership Agreement between Chile, New Zealand and Singapore[80] and the Comprehensive and Progressive Trans-Pacific Partnership,[81] aim to reduce trade barriers in the digital economy, build comparative standards, and promote regulatory harmonization in domestic legal frameworks governing electronic transactions and cross-border business.

Overall, if cross-border e-commerce is to deliver on its full potential, e-commerce issues must become an integral part of the trade policy agenda. There is an advantage to putting these provisions into trade agreements, since these agreements have a high public profile. These provisions can attract political attention in a way that technical law reform rarely does, which can generate the political will to implement them in domestic law.[82]

---

[77] Duval, Y. and K. Mengjing. 2017. *Digital Trade Facilitation: Paperless Trade in Regional Trade Agreements*. ADBI Working Paper 747. Tokyo: Asian Development Bank Institute. Available online: https://www.adb.org/publications/digital-trade-facilitation-paperless-trade-regional-trade-agreements.

[78] Monteiro, José-Antonio &Teh, Robert, 2017. "*Provisions on electronic commerce in regional trade agreements*", WTO Staff Working Papers ERSD-2017-11, World Trade Organization (WTO), Economic Research and Statistics Division, online https://ideas.repec.org/p/zbw/wtowps/ersd201711.html.

[79] Online: https://wits.worldbank.org/GPTAD/PDF/archive/Singapore-Australia.pdf.

[80] An overview with link to the official text are online: https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement.

[81] Online: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents.

[82] J.D. Gregory, "Trade Agreements to Promote Electronic Commerce", Slaw.ca blog: part I, 2016, online: http://www.slaw.ca/?s=trade+agreements+electronic+commerce ; part II, 2018, online:

1. Now in force in the Kyrgyz Republic

a. The World Trade Organization Trade Facilitation Agreement[83]

The WTO TFA requires contracting states to use e-communications for a number of domestic and international purposes. Parties are given time to comply with the requirements, depending on their state of economic development.

The Kyrgyz Republic has been a party to the WTO TFA since 1998. As a country classified as a developing economy, it has currently met just over 75% of its obligations to use paperless communications.[84] The delay, if any, is technologic – putting the systems in place – rather than legal, since the TFA itself provides the legal authority.

b. Revised Kyoto Convention

(World Customs Organization's International Convention on the Simplification and Harmonization of Customs Procedures (as amended)). The Kyrgyz Republic joined this convention in November 2021 (and will therefore need some time to adjust its practices to the new rules.)

The 2006 revision changed customs practice from inspecting every package to managing the risk of contraband and other unsuitable goods and promoted the use of electronic forms.[85]

c. Commonwealth of Independent States Free Trade Agreement

This agreement among several members of the Commonwealth of Independent States, including the Kyrgyz Republic, deals with a number of traditional trade issues but does not contain e-commerce provisions.

d. Other trade agreements:

The WTO has published a list of agreements to which the Kyrgyz Republic is a party, including agreements made by the EAEU that involve the Kyrgyz Republic as a member of that body.[86]

---

http://www.slaw.ca/2018/11/08/trade-agreements-to-promote-electronic-commerce-ii/; part III, 2019: http://www.slaw.ca/2019/12/30/trade-agreements-to-promote-electronic-commerce-iii/.

[83] World Trade Organization, Trade Facilitation Agreement, online: https://www.wto.org/english/tratop_e/tradfa_e/tradfa_e.htm.

[84] See the WTO table of progress in implementation, online: https://tfadatabase.org/implementation/progress-by-member.

[85] The Revised Kyoto Convention is described here: http://tfig.unece.org/contents/revised-kyoto-convention.htm. A guide to its provisions is here: https://www.wcoesarocb.org/wp-content/uploads/2018/07/1.-WCO-Revised-Kyoto-Convention.pdf.

In addition, the United Nations runs "Special programs for the economies of Central Asia" (SPECA), launched in 1998, which aims to facilitate economic cooperation in the SPECA region and integration of the SPECA participating countries[87] into the world economy, and to provide a platform for cross-border cooperation for the achievement of the Sustainable Development Goals.[88]

The US State Department lists a number of regional or bilateral trade agreements or investment agreements, including one with the United States.[89]

2. Potential trade agreements for the Kyrgyz Republic

a. UN/ESCAP Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific [90]

The agreement sets out principles of a rational, acceptable, harmonized approach to cross-border paperless trade. It encourages parties to the agreement to create a national policy on this trade, establish a single window to handle documentation destined for different agencies within the state, and set up systems to promote the mutual recognition of trade documents among member states (and other trading partners). Each contracting party is to take these steps, which all align with international best practices, in ways consistent with its own legal system and traditions.

The framework agreement encourages rather than requires actions, which allows ESCAP member states such as the Kyrgyz Republic to join no matter how ready they currently are to engage in cross-border paperless trade. The rules serve as guides for those at the early stages, and as confirmation of steps already taken for those more advanced in the process. They provide a path along which all the parties can work in a consistent way (but at their own pace) to facilitate their trade with each other and the rest of the world. ESCAP may also be able to offer resources to help parties to the agreement engage in cross-border paperless trade.

b. Regional Comprehensive Economic Partnership91

---

[86] WTO Regional Trade Agreements database, online: http://rtais.wto.org/UI/PublicSearchByMemberResult.aspx?MemberCode=417&lang=1&redirect=1

[87] The countries are Afghanistan, Azerbaijan, Kazakhstan, Kyrgyz Republic, Tajikistan, Turkmenistan, and Uzbekistan. SPECA is supported by the United Nations Economic Commission for Europe (UNECE) and the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). This description of SPECA is taken from the WTO Trade Review document referenced in footnote 97, below.

[88] UNECE and ESCAP, SPECA Terms of Reference, 2019. Viewed at: https://www.unece.org/fileadmin/DAM/SPECA/documents/gc/session14/V._SPECA_ToR_ENG_Final.pdf

[89] U.S. International Trade Administration: Kyrgyz Republic – Country Commercial Guide – Trade Agreements, online: https://www.trade.gov/country-commercial-guides/kyrgyz-republic-trade-agreements

[90] Source of information on the Framework Agreement are online: https://www.unescap.org/kp/cpta

The RCEP is a creature of the Asia-Pacific Economic Cooperation (APEC) organization that includes most significant Asian economies, including the People's Republic of China, the Republic of Korea, Japan, Singapore and Australia. It came into force on 1 January 2022 and is open for accession by any other "state or unit" in the region for 18 months.[92] The official text does not say what "the region" is for this purpose, but it is reasonable to assume that any Asian nation would be welcome.

While the RCEP does reduce tariff barriers among its members, it also contains a chapter on electronic commerce law and regulation.[93]Most of the chapter is in terms of "the parties shall endeavour" to achieve cooperation and harmonization in their laws and practices of e-commerce. They are obliged to have a legal framework "taking into account" the UNCITRAL Model Law on Electronic Commerce and the UN Electronic Communications Convention, and other model laws and international conventions relating to e-commerce. (article 12.10) They must also adopt recognized principles for consumer protection (12.7), privacy protection (12.8) and fighting unsolicited commercial messages (spam)(12.9). These provisions also stress enforcement of the rights given.

The rules on electronic signatures are as strong as any rule in RCEP (article 12.6).

> Except in circumstances otherwise provided for under its laws and regulations, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.
>
> Taking into account international norms for electronic authentication, each Party shall:
> (a) permit participants in electronic transactions to determine appropriate electronic authentication technologies and implementation models for their electronic transactions;
> (b) not limit the recognition of electronic authentication technologies and implementation models for electronic transactions; and
> (c) permit participants in electronic transactions to have the opportunity to prove that their electronic transactions comply with its laws and regulations with respect to electronic authentication.

---

91 Source materials on the Regional Comprehensive Economic Partnership (RCEP) are online: https://rcepsec.org/. The legal text is online:https://rcepsec.org/legal-text/.

92 RCEP, legal text, footnote 91, article 20.

93 RCEP, footnote 91, chapter 12, Electronic Commerce, online : https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf

However, some performance standards may be imposed on some kinds of signature under some circumstances (article 12.6(3)). In fact, most obligations in RCEP are subject to discussion or consultation based on overriding public interests in the member states, and rules or prohibitions turn out to be less absolute than their framing appears as a first impression.

In short, RCEP may give to the Kyrgyz Republic some allies in developing e-commerce practices, but probably its best use for e-commerce is in providing links for cross-border cooperation in enforcing rules on parties from outside the country.

B. Regional economic cooperation agreements

Agreements about regional economic cooperation may require the participating states to take legislative measures to express the cooperation, including in trade matters. They can be important in any event to the expansion of e-commerce among the parties, by allowing for discussions of matters of common interest, such as rules for cross-border flows of personal or economic information, cooperation in fighting cybercrime, and the like.

1. Now in force in the Kyrgyz Republic

a. Central Asia Regional Economic Cooperation (CAREC)

The CAREC Program unites eleven central Asian countries to promote regional development, notably in transportation, energy, and poverty reduction.[94]It has not engaged in notable work on electronic commerce, beyond publishing (with the ADB) a study in 2021 on e-commerce laws and regulation,[95] and very recently, a review of the technological infrastructure for e-commerce in member states.[96]Efforts to develop or harmonize those laws or that regulation have not followed, at least not coordinated or led by CAREC.[97]

b. Eurasian Economic Union (EAEU)98

[94] Central Asia Regional Economic Cooperation, online: https://www.carecprogram.org/.
[95] E-Commerce in CAREC Countries: Laws and Policies, ADB 2021, footnote 69.
[96] Footnote 3 above.
[97] The World Trade Organization describes CAREC as follows [footnotes omitted]: "… the Central Asian Regional Cooperation (CAREC), established in 1997, provides for project-based regional cooperation in the areas of trade, energy, and transport. It has 11 members and is supported by 6 multilateral institutions. CAREC's Integrated Trade Agenda 2030 aims to assist CAREC members with integrating further into the global economy and comprises three pillars: trade expansion from increased market access; greater diversification; and stronger institutions for trade. CAREC plays an important role in the development of regional and inter-regional transport networks." WTO Trade Policy Review (2021), online: https://docsonline.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/TPR/S411.pdf&Open=True.
[98] Eurasian Economic Union web site is online: http://www.eaeunion.org.

The EAEU was created in 2014 and now has five member states including the Kyrgyz Republic. It has developed uniform legislation that member countries adopt to facilitate trade within the Community. An early example is the Customs Code of 2018.[99]That law in turn affects economic infrastructure: the 2022 – 2027 draft Action Plan of the Cabinet of Ministers of the Kyrgyz Republic contemplated the creation of customs warehouses for goods located in border areas, "within the framework of the EAEU and in accordance with WTO requirements."[100]Moreover, current work is being done by the Customs Authority on exemptions from customs duties for personal importation of goods below a certain value (200 euros) and weight (31 kilograms), which are EAEU standards.[101]

The EAEU has been negotiating with Viet Nam about an electronic certificate of origin. Its arrangements on that point will apply as well in the Kyrgyz Republic.

Moreover, the nature of the Republic's membership will make some of the EAEU's rules mandatory when they are adopted. Work is being done, for example, on the operation of e-commerce platforms, with at least one such platform contemplated for each EAEU member state. See the provisions of the *Law about electronic commerce* on trading platforms mentioned above,[102] which may reflect the focus of the EAEU on the topic.

In addition, the Action Plan on e-commerce proposes to bring consumer protection laws into compliance with the requirements of the technical regulations of the EAEU, by the fourth quarter of 2022 (item 1). This is discussed further in the consumer protection part of Section V of this report.[103]

The EAEU is also developing, as mentioned earlier, its "transboundary trust environment" or "transboundary space of trust", a multi-year project. The work involves devising common legal, organizational and technical standards for trusted authentication of documents that would cross

[99] Customs Code of the EAEU, in force January 2018, online: http://www.eurasiancommission.org/ru/act/tam_sotr/dep_tamoj_zak/SiteAssets/Customs%20Code%20of%20the%20EAEU.pdf.
[100] Action Plan, footnote 2, item 8. The item no longer appears in the final version of the Action Plan.
[101] Conversation of Iskander Artykbaev with Customs officials, 23 March 2022.
[102] See text at note 15.
[103] See text at note 146.

borders in paperless trade. It would presumably lead to harmonizing of such standards among EAEU member states.[104]

It will be noted that this project has been going on for several years. Even among countries with much in common economically and politically, it is difficult work. One might conclude that short-cuts and less-than-perfect solutions to cross-border or cross-system authentication systems may provide the way to do business in the meantime.[105]

C. Instruments that expressly target e-commerce for its own sake

1. E-Commerce instruments now in force in the Kyrgyz Republic

a. UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures.[106]

These model laws represent the international state of the art for removing legal barriers to electronic commerce. The Kyrgyz Republic has not followed the Model Law in particular, though the 2021 *Law about electronic commerce*[107] seems largely to get to the same place for validity of e-transactions. It does not, as does UNCITRAL, make information in electronic form the functional equivalent of the information on paper, if certain conditions are met.[108]The operation of the 2021 statute was discussed in more detail earlier in this report.

b. Customs Convention on the International Transport of Goods under Cover of TIR Carnets (TIR Convention)

[104] See the brief discussion above under Trust Services, text at footnote 47. S.A. Kiryushin, "Methodology of formation of transboundary trust environment and the requirements for its creation, functioning and development," UNESCAP Proceeding October 2017, online: https://www.unescap.org/sites/default/files/Contribution%20Background%20Document_Methodology%20of%20TTE_0.pdf. See also the EAEU document showing the project, EEC Facts and Figures 2020, http://www.eurasiancommission.org/ru/Documents/3264_%D0%95%D0%AD%D0%9A_%D0%A6%D0%98%D0%A4%20-%202020_%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0%B8%D0%B5%20%D1%80%D1%8B%D0%BD%D0%BA%D0%BE%D0%B2%20%D0%B8%20%D1%86%D0%B8%D1%84%D1%80-%D0%B8%D1%8F_%D0%B0%D0%BD%D0%B3%D0%BB.pdf pages 10 – 12 (as numbered) Moreover, the transboundary trust environment notion is also mentioned as a general principle underpinning the Framework Agreement on Cross-border Paperless Trade in Asia and the Pacific, and the adoption of the Framework Agreement may facilitate TTE implementation.

[105] The EAEU also distinguishes between 'e-commerce' and 'paperless trade.' It may be worth ensuring that everyone has a common understanding of the principles being discussed. It may be thought that e-commerce is activity carried on via a platform of some sort, while paperless trade flows more freely through wired and wireless connections without oversight or intermediation by a platform. The terms are not differentiated outside Central Asia.

[106] Footnotes 7 and 19 above.

[107] Footnote 10 above.

[108] The official UNCITRAL lists of states that have implemented these model laws does not include the Kyrgyz Republic. See https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce/status and https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status

The Convention should be read with Annex 11 on digital documents (in force May 2021).[109]This Convention provides for mutual recognition of shipping forms among the many member countries. Annex 11 appears to come into force automatically, i.e. member states of the Convention do not have to take separate legislative action to have it apply.

2. Potential instruments on electronic communications

a. United Nations Convention on the Use of Electronic Communications in International Contracts (the E-Communications Convention or ECC).

This Convention restates many of the rules for e-communications in the UNCITRAL Model Laws. Article 20, para 2 of the Convention provides a method by which a contracting state may interpret other international commercial conventions to which it is a party, in the light of UNCITRAL's e-commerce principles. This avoids the need to have these conventions modified expressly to allow e-communications. (The main conventions of this type in the Kyrgyz Republic are the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards and the Convention on the International Sale of Goods.) This could extend the benefits of such communications to many legal international relationships of the Kyrgyz Republic.

Moreover, about 20 countries have used the substantive provisions of the E-Communications Convention as a template for their domestic law.[110]

b. UNCITRAL Model Law on Electronic Transferable Records

Adopted in 2017, the Model Law on Electronic Transferable Records provides an electronic functional equivalent to important trade documents that themselves suffice to transfer the value of the goods they describe or of a sum of money.[111] Examples are bills of lading and warehouse receipts. Possession of the document entitles the holder to possession of the goods or to payment of money, so there should be only one document giving this right for any set of goods. This Model Law overcomes difficulties in creating unique electronic records, relying on appropriate assurances (not just in words but in technology) that an authoritative version of the record exists and can be safely transferred electronically. The MLETR is in early stages of

[109] UN/ESCAP, Towards Electronic TIR Customs Transit System (eTIR), September 2014, online: https://www.unescap.org/sites/default/d8files/knowledge-products/brief12.pdf.

[110] There is also a respectable argument for harmonizing one's domestic e-commerce law with the ECC, to make all transactions on an equal legal footing. Singapore and Australia have done this, and it has been recommended for Canada. The engagement of public officers in the Kyrgyz Republic in identifying and authenticating its citizens online and in certifying their signature data might make such an integration more difficult.

[111] Model Law on Electronic Transferable Records, 2017, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

implementation around the world but should be kept in mind in a comprehensive e-commerce legislative strategy.

D. Other current treaties and related agreements

1. Treaties now in force in the Kyrgyz Republic

a. United Nations Convention on Contracts for the International Sale of Goods (CISG)

This convention, sometimes known as the Vienna Sales Convention, sets basic rules for the sale of goods between parties in different states. It was adopted in 1980 and does not expressly authorize electronic communications. However, the UN Convention on Contracts for the International Sale of Goods Advisory Council, a private group of experts on sales law, has found the convention to be consistent with electronic communications and to operate in the same way when they are used.[112]This conclusion is consistent with the general principle of freedom of form, upon which the CISG is based.

This could have important consequences for countries like the Kyrgyz Republic that are parties to the Convention, since the Convention applies automatically to international sales contracts unless the contracting parties opt out. In other words, the law mandatorily applicable to such contracts permits e-communications to make them. This could provide useful flexibility to businesses looking to do international sales with e-documents, especially in countries where international treaties prevail over domestic laws, which include most CAREC members.

Note: The multi-year action plan mentioned below (see section IV of this report) has implementation of CISG as an item. Nonetheless the official UN site for the Convention says that the Kyrgyz Republic is already a party.[113]The Action Plan (item #3) links the Convention to an OECD project on tax avoidance in the digital age, notably the understatement of the tax base and unreported withdrawal of profits from e-commerce sites.

b. Sanitary and Phytosanitary (SPS) Agreement

There are several treaties on the trade in plants, notably the International Plant Protection Convention from the World Food Organization (FAO) dating from 1951, and a World Trade

[112] UN Convention on Contracts for the International Sale of Goods-Advisory Council Opinion no. 1, Electronic Communications under CISG, 15 August 2003. http://www.cisgac.com/cisgac-opinion-no1/.

[113] United Nations Treaty Collection: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-10&chapter=10&clang=_en. See also the UNCITRAL website status page on theConvention: https://uncitral.un.org/en/texts/salegoods/conventions/sale_of_goods/cisg

Organization SPS agreement that interacts with the IPPC. The current versions allow or contemplate the exchange of information electronically. In particular, National Notification Authorities may now use the SPS Notification Submission System (SPS NSS) to fill out and submit SPS notifications.[114]

c. Convention on Trade in Endangered Species (CITES)

The Convention on International Trade in Endangered Species of Wild Fauna and Flora allows for electronic declarations of exemptions from trade bans using electronic forms.[115]The Kyrgyz Republic became a member in 2007.

2. Potential treaties to assist in e-commerce in the Kyrgyz Republic

a. International Convention on the Harmonization of Frontier Controls of Goods

This convention allows standard reference to products in trade, which makes standard forms and thus electronically readable documents easier.[116]

b. United Nations Layout Key for Trade Documents

The UN Layout Key is a document – not itself a convention, more of a standard as described in the next section - used in conjunction with the UN convention below to enable readers to understand forms even when the forms are prepared in a language that they do not comprehend.[117] The forms speak for themselves once they are standardized. The United Nations International Convention on the Harmonization of Frontier Controls of Goods makes the use of this layout mandatory for member states. The UN Centre for Trade Facilitation and

[114] See WTO web pages for information: https://www.wto.org/english/thewto_e/coher_e/wto_ippc_e.htm and https://www.wto.org/english/tratop_e/sps_e/sps_e.htm.
[115] Convention on International Trade in Endangered Species of Wild Fauna and Flora. 1973 (amended 1979 and 1983). Convention text. https://cites.org/eng/disc/text.php. See also https://cites.org/eng/disc/what.php for a description of the Convention.
[116] A description is here: http://tfig.unece.org/contents/Harmonized-frontier-controls-convention.htm and the text here: http://www.unece.org/fileadmin/DAM/trans/conventn/ECE-TRANS-55r2e.pdf
[117] http://tfig.unece.org/contents/recommendation-1.htm.

Electronic Business (UNE/CEFACT) says that the Layout Key "can also be used to design screen layouts for the visual display of electronic documents."[118]

E. International standards

1. Now available

a. UN Centre for Trade Facilitation (CEFACT) recommendations

These documents are not mandatory, as are conventions, but they provide internationally approved best practices for implementing workable rules or electronic trading. Its texts on the legal and administrative considerations in establishing a Single Window were mentioned above, as was the harmonized layout document. There is a large and useful collection of trade facilitation standards, grouped as recommendations.[119] Once they are incorporated into national law, however, they are mandatory according to the terms of that law.

b. International Standards Organization (ISO) standards

ISO standards have many applications for approaches to cross-border e-commerce. Among the most important are those affecting authentication certificates and information security - the 27000 series.[120]

IV. PROPOSED E-TRANSACTION LAWS

The Kyrgyz Republic has been actively reviewing its laws concerning electronic communications, both in commercial matters and in the relations between state and citizen. Some statutes are very recent: the *Law about electronic commerce* dates from December 2021 and came into force in May 2022. The *Law on consumer protection* was amended in January 2022. Some implementing regulations for other statutes are likewise quite new and untested. The Revised Kyoto Convention has been in force only since November 2021.

The *Law about electronic commerce* is enacted, as stated, but it contemplates rules and regulations that are not yet prepared. As a result, there may be questions about its application in some circumstances – through several of the general permissions in the statute, such as giving an electronic document the same status as one on paper, can have a beneficial effect without

[118] See the description of Recommendation 1 at: http://www.unece.org/tradewelcome/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/cefactrecommendationsrec-index/trade-facilitation-recommendations.html.
[119] UNE/CEFACT Recommendations on Trade Facilitation, online : https://unece.org/trade/uncefact/tf_recommendations.
[120] International Standards Organization, ISO/IEC 27001 Information Security Management, online: https://www.iso.org/isoiec-27001-information-security.html.

enabling regulations. Likewise, the exemption from intermediary liability will be attractive as offered on the face of the statute.

However, it is always worth asking if business people and their customers will feel free to transact electronically in the absence of a regulatory framework not yet enacted. [121]
It will not be possible in the short term to calculate with any accuracy the economic benefit of such permissions.

Meanwhile, we refer again to the recent "Action Plan of the Cabinet of Ministers to support and develop e-commerce in the Kyrgyz Republic for 2023-2026."[122] It sets out for discussion a number of areas for legislative attention. Some of the topics are mentioned in the Framework discussion below, such as consumer protection and personal data protection (privacy). Some have been mentioned earlier in this report: the legal framework for National Single Window; the creation of electronic certificates of origin, the design of customs warehouses in accordance with EAEU and WTO rules. Overall, it is an interesting and competent document.

Item 4 of the draft Action Plan discussed the regulation of e-signatures, with special attention to remote authentication and user verification systems. (The final version of the Action Plan did not include the e-signature item.) Remote authentication became especially important with the Covid pandemic, where traditional in-person signing sessions were often avoided. The applicable law needs to contemplate practical challenges: how can remote transacting parties, or remote legal witnesses (or even notaries), be sufficiently certain of the identity of the other parties? How can they be sure that what is being signed is what is supposed to be signed, or what is sent later? For notarization, how can one be sure that the person signing as notary is in reality a notary?[123] In short, reliable authentication is needed for the participants in the signing action – signatory and witnesses – and for the document(s) being signed, at the time of signing and at the time of later use.

---

[121] The e-Commerce Association of the Kyrgyz Republic submitted abrief proposing amendments to the *Law on electronic commerce*. Its specific proposals are dealt with throughout the text of this report.

[122] Footnote 2.

[123] The Law about electronic commerce excludes notarized documents from its scope. However, a number of places in the world are considering remote notarization – there is an established legal framework for it in the United States, for example. The questions raised are similar to those for other remote signing systems, so they should not be excluded in principle. The Ministry's draft Action plan (footnote 2) included a recommendation on remote signing, though that item was removed from the final version. See discussion in the Recommendation for Development section, text at note 210.

These questions have often been answered by legal requirements that remote signing be witnessed on a live video feed, with parties properly identified by special software that can verify the validity of identification documents like passports or driver's licenses. Digital signature systems can be set up to record each signature in order and prevent any alteration to the signed document once a signature is placed on it. Registers of notaries can be created for checking online in real time when verification is needed.

Moreover, the verification system already available under Kyrgyz law, using the Infocom system and relying on passport authentication, may be adaptable to remote usage. People can already enrol themselves for digital signatures without showing up in person. Using these signatures in anespecially secure way should be a relatively small step, at least conceptually, from where the country is now. It is possible that for remote use among private parties, signatories will need an enhanced e-signature rather than a simple one now distributed for free. (As noted earlier, there are questions of user comfort throughout the system, but they do not necessarily require law reform to resolve.)

A number of the Action Plan proposals are technical or practical (e.g. educating entrepreneurs, item 14) rather than legal.[124] Building an e-commerce platform to promote Kyrgyz goods and services internationally will not affect the law, except to the extent traders through that platform have special tax or customs clearance advantages.(item9)

Others promote integration into international efforts, such as proposed adhesion to the OECD's digital taxation program/strategy (item 3). The valuation of goods in commerce – physical and electronic – is a key issue in cross-border trade, as it affects customs duties and the basis for income and value added taxes. Valuation questions are complex, however, and require technical expertise beyond the scope of this report.

It will be noted that the Republic has decided to provide in calendar 2022 very low rates of all forms of taxation – sales tax, value-added tax on supplies, income tax – on sales conducted through electronic commerce.[125]Online sellers and operators of trading platforms all benefit from

[124] The Asian Development Bank's project of which this study is a part also includes a set of teaching materials – videos and slides – on how to run an e-commerce business. The results are online on the website of the CAREC Institute: https://elearning.carecinstitute.org/e-commerce.

[125] See *Tax Code*, Kyrgyz Republic, chapter 61, articles 443 to 449, enacted 22 December 2021. Online: http://cbd.minjust.gov.kg/act/view/ru-ru/112340?cl=ru-ru. The reduced rate does not affect customs duties; cross-border transactions remain taxed at their usual rates.

a 2% tax rate on domestic sales. The E-Commerce Association of the Kyrgyz Republic had further proposals for tax advantages for those engaging in e-commerce.[126]

A taxpayer with mixed sources of income (some from e-commerce, some not, or some from domestic transactions and some from foreign ones) is required to calculate and pay tax separately from the different income streams at their appropriate rate. These calculations may be difficult to make and even harder to enforce in practice. Will there be a temptation by business people and/or tax officials to make private arrangements to resolve such questions?

The government should ensure that e-commercial activities are handled consistently as between the Law on e-commerce and the Tax Code. The e-Commerce Association mentioned in particular expanding and synchronizing the scope of Art. 443, p. 1 of the Tax Code and Art. 8, p. 1 of the Law on Electronic Commerce.[127] It also mentioned participating in an OECD working group on valuation of goods in cross-border trade for tax purposes.[128]

Devising incentives to attract foreign direct investment from e-commerce businesses (item 9) is also beyond the scope of the present analysis.

V. FRAMEWORK AND CONTEXT FOR ELECTRONIC COMMERCE[129]

Foreword on Regulation

The section on Electronic Transactions at the beginning of this report reviewed UNCITRAL's work aiming to enable electronic transactions in a world full of requirements designed for paper documents. While the work was useful, as shown by its widespread adoption around the world, it did not claim to be everything a legal system would need in order to support electronic communications. UNCITRAL's silence on regulatory matters was not an assent to existing rules or a statement that nothing more was needed to facilitate electronic commerce.[130]

It has become clear, if it was not always clear, that the successful spread of electronic commerce in a society depends on a number of factors. The technology has to be available, the

[126] Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 2.
[127] Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 2.
[128] Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 5. The OECD project is developing a comprehensive framework on combating understatement of the tax base and profit shifting in digital taxation. See the discussion of the Ministry's Action Plan, below, Section VI.B.4.
[129] Much of the explanatory text in this section is taken or slightly adapted from the principal author's report on CAREC E-commerce legislation published in 2021 by the ADB. Footnote 69.
[130] See Guide to Enactment, MLEC, footnote 7, paragraphs 13 - 14

means to generate, receive and transact with electronic documents. The best enabling law will not build a computer where none exists or teach someone to use it once built. The host economy has to be rich enough and vibrant enough to support innovation, since some attempts to launch e-businesses will fail.

Another very important, though intangible, factor is that people must be willing to trust e-commerce: the technology and the people. Is it too risky to venture onto a computer, onto the Internet? Who and what is out there?

Trust has many facets. It is a kind of judgment about future conduct. In a trustworthy society, people keep their word, fulfil their contracts, act properly, because that conduct is expected. If this is not so in the physical economy – if people are fearful to engage in transactions with strangers – then it may be even more difficult online, where one cannot see the people one is asked to deal with.

On the other hand, some measures of cyber security can make electronic transactions more trustworthy than dealings in person. E-commerce transactions may be more transparent and auditable than traditional in-person interactions. This is a trustworthiness that needs to be demonstrated and learned, however.

Recently the Asian Development Bank and the United Nations Economic and Social Commission for Asia and the Pacific (UN/ESCAP) published a study of the spread of e-commerce in Asia.[131] They observed that the development of e-commerce depended on economic factors and conditions, the legal and institutional environment, and social acceptance and awareness.[132]

These three dimensions were inter-related; they all affected each other, and it was hard to arrive at mature e-commerce in society without all three being in good shape.

It is beyond the scope of this Report to evaluate the Kyrgyz Republic's state of economic development or degree of social trust. However, there are legal measures besides UNCITRAL's enabling of electronic transactions that can build economic trust, that can make e-commerce

[131] *Embracing the e-Commerce Revolution in Asia and the Pacific,* June 2018, footnote 4. The document includes examples from several CAREC member states.
[132] Ibid, p 13.

appear safer and more appealing to potential businesspeople and their potential customers. The ADB/ESCAP study and several others[133] consistently mention the legal and institutional framework of e-commerce, and the consistent content of that framework includes rules of privacy, consumer protection and online security, i.e., protection against online crime. These are crucial elements of trust and thus of growing e-commerce.[134]

A useful overview of principles, particularly but not solely devoted to consumer protection in e-commerce, was published in 2021 by US AID: *E-Commerce Code of Conduct: Recommendations for e-commerce development in Central Asia*.[135]Its contents are consistent with the rest of the present report.

This section of the Report will review the legal elements of these three and other topics and describe the best practices for a regulatory framework that the Kyrgyz Republic could consider in order to promote e-commerce. The country has made notable progress in many fields, but more could still be done in some cases, and efforts to harmonize what they have done or will do can help build regional growth through electronic means.

A final word of background: regulatory measures depend on the ability of the state to administer and enforce them.

- One may recommend consumer protection measures, but is the government capable of running a consumer services bureau and helping the people who need it? Is there a trusted court system or other dispute resolution process available to people whose new rights are not respected?
- One may recommend privacy laws requiring informed consent and high standards of secure storage of personal data, but can the state afford and find or train inspectors to check that the laws are being followed, and officials to compel compliance if the inspectors find it deficient?
- One may recommend strict measures against cybercrime – unauthorized access to computers, spreading malware – but does the state have the technical expertise to

[133] For example, see UNCTAD, *Rapid e-Trade Readiness Assessments of Least Developed Countries: Policy Impact and Way*, (2019), online: https://unctad.org/en/PublicationsLibrary/dtlstict2019d7_en.pdf;UN/ESCAP, *Digital and Sustainable Trade Facilitation: Global Report* 2019, online: https://untfsurvey.org/report.

[134] That said, laws to remove legal barriers to the use of e-communications can also be seen as building trust, especially where the law touches on authentication. See John D. Gregory, "Legislating Trust" (2014), 12 *Canadian Journal of Law and Technology* No.1, 1. Online: https://digitalcommons.schulichlaw.dal.ca/cjlt/vol12/iss1/1/

[135] US AID, 2021. Copy in possession of the authors.

follow cybercriminals through the “darknet” and around the world to put an end to this activity?

A. Consumer protection

International best practices
A good source of inspiration for consumer protection principles are the United Nations Guidelines for Consumer Protection, most recently updated in 2015.[136] Member states should establish consumer protection policies that encourage:

- Good business practices
- Clear and timely information for consumers to contact businesses
- Clear and timely information about goods and services sold
- Clear, concise and easy to understand – and fair – contract terms
- A transparent process for cancellation, returns and refunds
- Secure payment mechanisms
- Fair, affordable and speedy dispute resolution
- Consumer privacy and data security
- Consumer and business education

Moreover:

- Consumer protection agencies should have adequate resources
- Goods should be safe for intended or foreseeable uses
- Manufacturing should be sustainable.

The main Kyrgyz *Law on consumer protection* dates from 1997, but it was last amended in early 2022.[137] It is a comprehensive and modern statute that sets out in detail the rights and duties of sellers (of goods and of services) and of consumers. It addresses the quality of goods (and

[136] Online: https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf.
[137] *Law on consumer protection*, December 10, 1997 No. 90, online: https://cis-legislation.com/document.fwx?rgn=357.

services), threats to health and safety arising out of them, problems of delivery, timing and payment, and other issues.

The Law provides for enforcement in a number of ways, including through adjustments in price and penalties for non-performance by sellers. It authorizes the establishment of the Coordination Council for the Protection of Consumer Rights, a body set up in 2003 and re-established in 2018.[138]Its main task is the implementation of coordinated actions of state administrative bodies and public consumer associations.

The Council is also a policy body – it advises, for example, on potential legislation and,among other things, on harmonizing Kyrgyz law with law of the European Union.

The Law also requires sellers to install equipment designed to accept payment through bank payment cards, electronic money, and barcode and QR symbols.[139] This Decision sets out a schedule of implementation for municipalities across the country.

In addition, the usual criminal law prohibitions against fraud, forgery and misrepresentation would apply to consumer transactions as to others.

Moreover, the *Law about electronic commerce* of 2021 includes as a principle of electronic commerce“ protection of consumer rights.”[140]Many of the obligations of sellers in article 5 of the Law are typical consumer protection measures around the world, such as:

- Disclosing online the seller’s legal name and contact information and payment procedures
- “Ensuring the right of consumers to receive information about goods and services”
- Not misleading buyers with false information about sales or reviews and ratings
- Ensuring the delivery of goods or provision of services in the agreed manner and at the agreed time
- Assuming the risks associated with ensuring the delivery of goods or provision of services;

[138] Order of the Ministry of Economy dated September 11, 2018, No.113, “On approval of the regulation on the coordination council for the protection of consumer rights”, online: https://cis-legislation.com/document.fwx?rgn=110142.
[139] Decision of the Government of the Kyrgyz Republic, “On consumer protection measures”, December 23, 2015, no. 869, (amended 24 December 2020), online: https://cis-legislation.com/document.fwx?rgn=84074.
[140] Footnote 10, article 4(3).

- Providing contracts and history of transactions at the request of participants in an electronic transaction.

The duties of a "trading platform operator" in e-commerce include "protecting the interests of consumers."[141] The OECD has published an analysis of online marketplaces and consumer protection as well.[142]The buyer in an electronic transaction has the right to obtain "complete and reliable information about the good and/or services offered for purchase", and "protection of their rights in accordance with the legislation of the Kyrgyz Republic in the field of consumer protection."[143]

These and the other obligations under the statute are enforceable "in accordance with the criminal law and the legislation of the Kyrgyz Republic on misconduct and violations."[144] It is not clear whether the Co-ordination Council created under the *Law on consumer protection* would have jurisdiction for these offences.

The Co-ordination Council has a short track record at present.

The "Action Plan of the Cabinet of Ministers to support and develop e-commerce in the Kyrgyz Republic for 2023-2026"[145] sets out for discussion a number of areas for possible legislative attention over the next several years. The first on the list is "amendments to the legislation in the field of consumer protection," in principle scheduled for the fourth quarter of 2022. The proposed contents include having a register of online stores, making available indications of the safety of products sold, protection of the local market from inferior products, and notification of compliance with technical requirements of the Eurasian Economic Union (EAEU).[146]

---

[141] Footnote10, article 6 (4) e).

[142]OECD, "The role of online marketplaces in enhancing consumer protection", April 2021, online: https://www.oecd-ilibrary.org/science-and-technology/the-role-of-online-marketplaces-in-enhancing-consumer-protection_ddca0e2e-en. The OECD also has material on consumer protection online in general. See "Recommendation of the Council on Consumer Protection in E-commerce", 2016, online:https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422

[143] Footnote 10, article 7(1).
[144] Footnote 10, article 20.
[145] Footnote 2, above.
[146] The Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 3, supports these goals.

The EAEU mentions the need for consumer protection right in its constitutive Treaty of 2014. It relies heavily on full disclosure of product and risk information to potential consumers, along with serious enforcement capacity. A detailed description of its approach was published in 2017.[147] All member states are required to conform to its principles and report to the EAEU Commission on progress in doing so. The US State Department reported in 2021 that "[Kyrgyz] regulations are still being harmonized" with EAEU standards.[148] A recent study by the International Trade Center of the United Nations, aimed at assessing the Kyrgyz Republic's technical and legal readiness for cross-border paperless trade, also indicated that harmonization was a work in progress.[149]

There is also a suggestion that privacy matters could be addressed from the perspective of consumer protection, though the topic is treated separately in the present report.

[147] "How the Eurasian Economic Commission Works in the Field of Consumer Protection", online: https://potrebitel.eaeunion.org/en-us/Pages/eec.aspx.
[148] U.S. Department of State, "2021 Investment Climate Statements: Kyrgyzstan", online: https://www.state.gov/reports/2021-investment-climate-statements/kyrgyz-republic
[149] UN International Trade Centre, Ready4Trade Central Asia, *Report on the assessment of the level of readiness of the Kyrgyz Republic for cross-border paperless trade*, DRAFT English text, 2022.

Conclusion and recommendation on consumer protection

The *law of the Kyrgyz Republic on consumer protection* is largely consistent with international best practices. It should be administered in a way that consumers are aware of their legal rights and have a practical, affordable and timely means to enforce them. Co-ordination with the rules of the EAEU – the closest trading partners of the Republic for many purposes – once they are available, can only improve the effectiveness of the standards to be applied.

B. Privacy (personal data protection)

International best practices

Early privacy guidelines were published by the Organisation for Economic Co-operation and Development (OECD) in 1980.[150] These guidelines have been made law in whole or in part by many countries to establish the following fundamental principles:

(i) collection limitation (no more information should be collected than is needed for the purpose disclosed to the person providing the information),
(ii) data quality (the information should be as reliable as possible),
(iii) purpose specification (the data collection must disclose to the data provider the purpose of the collection and proposed use of the data),
(iv) use limitation (the data should not be used for any undisclosed purpose),
(v) security safeguards (the data should be kept and managed securely),
(vi) openness (the practices and policies of the data collectors should be knowable to thosethey affect),
(vii) individual participation (the people whose information is being collected and used should have the right to know what information is held and to have it corrected if appropriate), and
(viii) accountability (there should be an effective remedy for an individual for any breach of these rules by the data collector or user).

The OECD revised the guidelines in 2013, while retaining many of the original principles.[151] Among the significant changes were greater emphasis on implementing and enforcing the

[150] OECD. 1980 (amended 2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. See also the convention to give stronger effect to the Guidelines: Council of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108; and Council of Europe. 2018. *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. https://www.coe.int/en/web/data-protection/convention108/modernised.

principles and a focus on the cross-border flow of personal information that reflects the advances in global information networks and the economic value of data.

The General Data Protection Regulation (GDPR) of the European Union (EU) came into force in 2018.[152] The GDPR not only governs the internal data practices of the EU, one of the world's largest economies, but the regulation also has spillover effects by applying to the personal data that EU member states transfer to the rest of the world. Data collection by international companies in the EU is also governed by the GDPR. The basic obligations that the GDPR imposes on data controllers in the public and private sectors are largely consistent with those that the OECD originally published in 1980.

Privacy is protected in the Kyrgyz Republic principally through the *Law about personal information*.[153]

This is a modern and comprehensive statute with the usual features of such legislation:

- Personal data is collected only with consent of the data subject, with certain standard exceptions such as public records, need for public health information, and the like.[154] A very detailed Order of the government spells out procedures for determining consent and notifying subjects of the transfer of their information to third parties.[155]
- Some sensitive information (health, religion, sexual preference) is subject to stricter controls and fewer exceptions to consent.[156]
- Personal information stored for archival, historical, statistical purposes and the like must be depersonalized.[157]
- Collection is limited to purposes disclosed at the time of collection and shall not be kept longer than that purpose requires.[158]

---

[151] OECD. 2013. *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[152] European Parliament and Council of European Union. 2016. *General Data Protection Regulation*. https://gdpr-info.eu/ and https://eur-lex.europa.eu/legal-content/EN/ TXT/PDF/?uri=CELEX:32016R0679&from=EN. The GDPR replaced the influential EU Data Protection Directive of 1995.
[153] *Law about personal information* (2008) No. 58, online: http://cis-legislation.com/document.fwx?rgn=22274#A000000012. Translation of the Kyrgyz statutes from Russian has occasionally been modernized by GoogleTranslate from what appears in the CIS database. The CIS title for this statute is"*Law about information of a personal nature*."(Note also that the statute was further amended in 2021 but in such a minor way as to make no difference to this review.)
[154] Footnote 153, articles 5, 9, 27.
[155] Order No. 759 about approval of procedure on receipt of consent, etc (2017), online: http://cis-legislation.com/document.fwx?rgn=102361.
[156] Footnote 153, article 8.
[157] Footnote 153, article 26.
[158] Footnote 153, articles 4.2, 4.4.

- "Arrays" of personal data (databases, archives) must be registered with the state, the statute prescribing a number of items of information to be included.[159]
- Personal data in arrays must be kept secure.[160] A detailed order of the government goes into considerable detail on how to do this.[161]
- The data subject has the right to access his or her personal data in an array and to have it corrected, updated or removed if the evidence supports such a step.[162] The right to removal seems to apply only in cases of wrongful collection or error, and not to constitute a right to be forgotten in the European sense.[163]

To enforce the *Law on personal information*, an "authorized state body" mentioned in the Law is supposed to ensure compliance with the Law.[164]The authorized state body is named in a regulation under the Act.[165]Appendix 1 of the regulation names the authorized state body as "The State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic". That regulation spells out its duties in some detail – essentially policy development and enforcing compliance with the *Law on personal information*. It can also coordinate with foreign privacy officials. Since this regulation was made only a few months ago (December 2021), there is little experience to judge how it may work.

The "Support Program and e-commerce development in the Kyrgyz Republic for 2023 – 2026" was published along with the Action Plan discussed in this report.[166] It analyses the economics and technology available for e-commerce in the Republic. After a detailed review of the challenges of privacy protection, it concludes that "the main problem associated with ensuring compliance with the provisions of the legislation on personal data – the lack of a clear understanding of what organizational and technical measures are necessary and sufficient to ensure that there are no grounds for holding the operator liable for violation of the requirements

[159] Footnote 153, article 30.
[160] Footnote 153, articles 6.2, 17, 21.
[161] Order No. 760 about approval of requirements for security and personal data protection etc (2017), online: http://cis-legislation.com/document.fwx?rgn=102362.
[162] Footnote 153, articles 10, 11, 12, 28.
[163] Footnote 153, article 19.
[164] Footnote 153, terms and definitions, article 3.
[165] About the State Agency for the protection of personal data under the Cabinet of Ministers of the Kyrgyz Republic, December 22, 2021, No. 325, online: https://cis-legislation.com/document.fwx?rgn=137323.
[166] Footnote 2.

of the law."[167] A business that wants to comply with privacy law may not be able to figure out how to do it with confidence.

The Support program document does not offer a solution to this problem. Having the state or business groups provide explanations of the rules and examples of their application would seem to be a good start.[168]

The recent *Law about e-Commerce*[169] also contains provisions that protect privacy. For example, among the duties of the seller in article 5 are:

- (12) provide an opportunity to search, correct, delete data of a personal and commercial nature obtained during an electronic transaction;
- (13) provide information on the methods, procedures for searching, correcting and deleting data of a personal and commercial nature obtained during an electronic transaction.

Article 6(4) requires the trading platform operator to provide for:

- (c) the procedure for deleting personal and commercial data of the seller from the platform;
- (e) protecting the interests of consumers and information of a personal and commercial nature.

The text of the privacy legislation, as supplemented by the law on electronic commerce, is largely satisfactory. It appears that the State agency that is to enforce the statute should do some educational outreach to the businesses that do not understand how to comply with the law with confidence.

Moreover, the e-commerceAction Plan (item 2, for 4th quarter 2023) foresees "stricter requirements" for the protection, processing and storing of personal information"obtained as a

[167] "Support Program and e-commerce development in the Kyrgyz Republic for 2002-2027", provided by the Ministry, footnote 2, page 5.
[168] The e-Commerce Association of the Kyrgyz Republic advocates ensuring that the privacy rules apply clearly to e-commerce, and also that personal data collected in the Republic remains in the Republic. Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2022, paragraph 4.
[169] Footnote 10.

result of e-commerce transactions."[170] So much data can be extracted from apparently simple online transactions that merchants may overstep the legal bounds without wanting to do so.

Moreover, a number of consumers, particularly perhaps outside urban areas, are very worried about threats to their privacy, despite the text of the legislation. This deters them from engaging in online transactions.[171]

Cross-border transfer of personal data

The law allows for cross-border transfers of personal information if there is a treaty with the destination country ensuring an equivalent level of protection for the information. If there is no treaty or no such level of protection, then transfer may occur only with the consent of the data subject or if it is needed for protection of that person's interest or if the information is in a public array of personal data.[172] However, the Support Program document says that foreign investors "are free to transfer customer data or other business-related data out of the country" (but perhaps not personally identifiable information.)[173]

The Action Plan also says that the law will be amended to require data localization, i.e., personal data of citizens of the Kyrgyz Republic will have to be stored in the country.[174] While such requirements may have some political appeal from the point of view of national pride, they can be costly for international merchants that need to set up separate databases in many countries. Free trade agreements sometimes ban or at least discourage such provisions as a result.

C. Data protection (commercial and official data)

"Data protection" is a comprehensive term including data security, data availability, and access control.It extends beyond data privacy or the protection of personal information as just discussed.

[170] Action Plan, noted in Footnote 2 above.
[171] Conversation of Iskander ArtykbaevMarch 2022 with Kubanychbek Shatemirov, the former Deputy Chairman of the State Committee for Information Technologies and Communications (now the Ministry of Digital Development).
[172] Footnote 153, article 25.
[173] Support program, footnote 2, p. 8.
[174] Footnote 2, item 2.

> Data protection is focused on protecting assets from unauthorized use, while data privacy defines who has authorized access.
> Data protection is the act of safeguarding the data already obtained, no matter what it is (personally identifiable information, payment data or proprietary/commercial information).[175]

Kyrgyz law has a number of ways of protecting such data in any event:

- Trade secrets are protected by law. The main evidence found on this point is the exclusion of such matters from the access to information statutes discussed below.
    - The *Law on guarantees and freedom of access to information* excludes "information containing state, commercial or official secrets" and the *Law on access to information held by state bodies…* excludes "secrets protected by law (commercial, banking, notarial, medical, lawyer, etc.)" (article 5 (2) 4) The *Law on e-governance* says (art 13(2) 3)) that confidential information includes information …. constituting a commercial secret. So there is some reasonable expectation of protection of trade secrets. That protection is presumably enforced by some free-standing action, not just by enforcement of exceptions to disclosure legislation.
- Intellectual property law: by which use or copying of somebody else's data is prohibited. Chapter 6 of the *Law about e-commerce*[176] deals with protecting intellectual property rights by the seller, by a trading platform and by intermediaries. It provides a system by which IP rights holders may notify the seller, the platform operator or the intermediary of its rights and the recipient must cease the violation.
    - In addition, the *Law about legal protection of programs for electronic computers and databases*[177] (1998 am 2020) deals with copyright in computer programs and databases, though it does not protect data more broadly than that.
- Cybercrime law: the *Criminal Code* of the Kyrgyz Republic prohibits unauthorized access to computer systems and the alteration of any data in those systems.[178]This prohibition would extend to ransomware attacks.

---

[175] *Forbes* magazine, "Data Privacy vs Data Protection: Understanding the distinction in defending your data," online : https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/?sh=281a6f6d50c9.

[176] Footnote10, articles 17 – 19.

[177] Law about legal protection of programs for electronic computers and databases, 1998 No. 28, amended 2020, online:https://cis-legislation.com/document.fwx?rgn=234.

Traditional laws protecting commercial and official data from interference or theft are generally media-neutral, so they would normally apply to electronic data. Beyond the separate *Law on the protection of state secrets of the Kyrgyz Republic,*[179]there seems to be little free-standing specific protection of commercial data. Nothing in the privacy statute described in the last section extends beyond the personal information of individuals to cover other data.

It appears likely that the Kyrgyz Republic should legislate more clearly to actively protect the confidentiality of any data – commercial or personal – that is not in its usual state accessible to the public. Such legislation could be similar to the *Law on Personal Information*, but it should prohibit the collection, use or disclosure of commercial or other confidential information except by express consent of the owners of the information (and such consent for commercial purposes may not be unusual among companies doing business together)[180] or by overriding public purposes.

At present there is no clear international best practice on the topic that could be imitated, but data protection laws are in place elsewhere and can be used as models for the Kyrgyz Republic.

[178] Criminal Code, articles 289 (general information) and 291 (specially protected information), online: https://www.legislationline.org/download/id/4221/file/Kyrgyzstan_CC_1997_%20am_2006_en.pdf.
[179] Law about the protection of state secrets in the Kyrgyz Republic, 2017 No. 210, online:https://cis-legislation.com/document.fwx?rgn=103019.
[180] Such consensual sharing may be limited by laws protecting competition and prohibiting collusion against the interests of customers.

International best practices:[181]
Freedom of information legislation should be guided by the principle of maximum disclosure.
Public bodies should be under an obligation to publish key information.
Public bodies must actively promote open government.
Exceptions to the right to access information should be clearly and narrowly drawn and subject to strict "harm" and "public interest" tests.
Requests for information should be processed rapidly and fairly and an independent review of any refusals should be available.
Individuals should not be deterred from making requests for information by excessive costs.
Meetings of public bodies should be open to the public.
Laws which are inconsistent with the principle of maximum disclosure should be amended or repealed.
Individuals who release information on wrongdoing – whistleblowers – must be protected."

D. Transparency of public information (access to official information)

Public access to information is provided by three statutes in the Kyrgyz Republic: the *Law on guarantees and freedom of access to information*,[182]the *Law on access to information held by state bodies and organizations*[183] and the *Law about e-governance*.[184]

The basic rules are in the *Law on guarantees and freedom of access to information*:

- Everyone is guaranteed the right of access to information (article 3)
- The state protects the rights of everyone to search, receive, research, produce, transmit and disseminate information, subject only to restrictions established by law (article 3)
- Everyone is entitled to make a request for information, though the law does not say to whom this request is to be made. Presumably it is made to whoever is custodian of the information. A list of bodies obliged to disclose the kinds of information they have appears in article 6. It includes state and local government bodies, public associations, enterprises, institutions, organizations and officials – so just about everybody beyond private individuals. Information is to be provided free where it affects "the rights and

[181] Article 19 Committee, International Standards: Right to Information, 2012. Online: https://www.article19.org/resources/international-standards-right-information/. See also United Nations, Economic and Social Council, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", 2000, online:https://www.refworld.org/docid/3b00f3e10.html . Moreover, the Council of Europe has a Convention on Access to Official Documents (2009), online: https://rm.coe.int/1680084826.

[182] *Law on guarantees and freedom of access to information*, 1997 No. 89, amended 2017, online:https://cis-legislation.com/document.fwx?rgn=100.

[183] *Law on access to information held by state bodies and organizations*, 2006 No. 213, amended 2017, online: https://cis-legislation.com/document.fwx?rgn=14692. A critique of this statute before its enactment was published by the access advocacy group "Article19", October 2006, online: https://www.article19.org/data/files/pdfs/analysis/kyrgyzstan-foi-06.pdf.

[184] *Law on e-governance*, footnote 42.

legitimate interests of the applicant"; otherwise its provision may be subject to a fee. (article 7)

- The requirement of openness does not apply to "confidential information, as well as information containing state, commercial or official secrets." (article 8) Article 10 describes information excluded – "not allowed in the media' – such as state and commercial secrets, information that might harm public order or encroach on the honor or dignity of a person or that is knowingly false.

The *Law on access to information held by state bodies and organizations* sets out rules as stated by its title. The bodies and organizations are defined in a straightforward way.

According to article 3, "the main principles of freedom of access to information are general availability, objectivity, timeliness, openness and reliability of information."

Article 5 sets out the restrictions on access, including the protection of the rights and freedoms of other persons (article 5(1) 3)). Access restriction is also established for information "containing secrets protected by law (commercial, banking, notarial, medical, lawyer, etc.)." (article 5(2) 4)).

Much of the rest of the statute describes procedures for getting access to different kinds of information from different sources, and the obligation of state bodies to publish information at their own initiative. Some procedural objections appear in article 15. The statute also sets out rules for the online publication of state-held information. It has long lists of information to be published, with details on the kinds of personal information to be edited out of such information (notably for court proceedings.)

For example, state bodies are obliged to create websites for posting official information (article 25). Meetings of state bodies are presumed to be open unless discussing matters made confidential by article 5 (article 26).

The third relevant statute, the *Law on e-governance*, is the most recent, though all three were amended to coordinate their provisions about five years ago. It contains the following provisions:

- Article 12 says that information is public if not limited by law or by decision of the owner of the information (It is not clear how big an exception "the decision of the owner" is. It may be a question of intellectual property.)
- Article 12 also says that information published in a format that allows public use is open data (sub 4)
- Article 13 excludes information designated as confidential, but the reasons for so designating it must be "proportional" to its importance.
- That article sets out categories of information deemed confidential (besides info designated by the owner as confidential). This list is not surprising.
    - It also includes a number of kinds of information that cannot be kept confidential, including about natural disasters or threats to public health, environmental issues, activities of state bodies etc.
- Article 14 describes various modalities of distribution, the need to publish information about the publisher so a person mentioned can attempt to have publication blocked.
- Article 15 requires state bodies to give access to information. People wanting access do not have to say why they want it.
- Article 21 refers to the state portal of electronic services that has been discussed earlier in this report.[185]

The three statutes in combination seem to provide the basic rules and administrative applications needed for an open system of public and relevant private information. There are no obvious gaps or failures from the point of view of international principle, except perhaps the final point of the list in the text box at the outset of this section: the protection of "whistleblowers" who disclose information not otherwise permitted to be make public, where the public interest in its disclosure overrides the interest in its secrecy. Such a provision can be an important safety valve in an information system, i.e. it can prevent the usual rules from working an injustice or a harm to the public interest. Justified whistle blowing may be rare but it is worth providing for.

The final provisions of the *Law on access to information held by state bodies* require proposals for "bringing legislative acts in line with this Law" and "aimed at solving organizational measures arising from this Law," as well as ensuring the Law's proper operation across national and local governments. (article 37(2)) The authors of the present report have not determined if these final

[185] See text at footnote 62for discussion of the state portal of electronic services.

provisions have been carried out or whether organizational or administrative gaps prevent the full operation of the Law as it was enacted.

It may also be noted that the Kyrgyz Republic is a member of an international consortium of governments that make draft legislation available online: the Open Government Partnership. The portal with upcoming legislation was created by decree in 2018. It contains government bills, draft by-laws, and – interestingly – citizens' proposals for law reform.[186]The site itself provides means for anybody to give feedback on any of the proposals. (One has to register with the site to give feedback, though not to read proposals or discussions. So there is some possibility to screen the origin of comments.)

E. Cybercrime and cybersecurity

International best practices

The standards are set by the Council of Europe's Budapest Cybercrime Convention (2001)[187]:

- Prohibit any unauthorized access to a computer system
- Prohibit any unauthorized interception of non-public transmissions of computer data
- Prohibit the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- Prohibit the intentional and unauthorized hindering of the functioning of a computer system
- Prohibit the unauthorized possession or sale of devices capable of committing the above offences or of computer passwords or access codes.
- Prohibit computer-related forgery and fraud
- Prohibit a wide range of activities related to child pornography
- Provide effective remedies against infringement of copyright.

[186] The open Portal is online:http://koomtalkuu.gov.kg/ru.

[187] Council of Europe. 2001. *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. An official explanatory note is also available online: https://rm.coe.int/16800cce5b.

Another vital ingredient of public confidence in e-commerce is an expectation of honest conduct online.[188] This study assumes that the Kyrgyz Republic has basic criminal laws in place prohibiting the usual forms of dishonesty, such as misrepresentation, fraud, forgery, and theft. Some countries also have competition laws meant to inhibit the creation of monopolies and monopoly-like conduct through such activities as price-fixing, price discrimination, and bait-and-switch selling. These laws are generally media-neutral: they apply to online and offline transactions equally. New legislation is not usually needed.[189] Adding protections that cover online crime specifically aims to bolster the trust of consumers and business participants in e-commerce.[190]

The essential provisions of laws against cybercrime are widely agreed. The two treaties on the topic—one in place, one in draft form—have many common elements but take different approaches to administration. The Council of Europe Convention on Cybercrime (Budapest Convention of 2001) is very clear on the application of criminal law to online activity.[191] It aims to ensure that the 47 Council of Europe member states, and any other states that choose to be

[188] The general discussion here is drawn from the 2021 ADB study of the CAREC countries. Footnote 69 above.
[189] Moreover, the Budapest Convention of 2001 requires that member states ensure that many traditional offenses remain offenses when committed online (see footnote 187).
[190] One study in Azerbaijan found that passing information security (cybercrime) legislation "was a critical driver of increasing consumer confidence." Asian Development Bank (ADB). 2016. A Snapshot of E-Commerce in Central Asia. *Asian Development Blog*. 18 January. https://blogs.adb.org/blog/snapshot-e-commerce-central-asia.
[191] Council of Europe. 2001. *Convention on Cybercrime*. Footnote 187.

inspired by the Convention, ban certain kinds of undesirable online conduct that might not be illegal under traditional law.[192]

The main online offenses that Convention signatories are required to prohibit are illegal access to information systems (computers and networks), illegal interception of computer communications, interference with data or systems, and the misuse of electronic devices. The offenses expressly include the creation and spread of malware that harms the ability to use one's computer and that may steal valuable information. This includes viruses, worms, ransomware, and the like.

A draft treaty prepared by the Russian Federation contains a list of offenses to be created by national law that is neither surprising nor particularly controversial and is in fact very similar to that of the Budapest Convention. It also protects copyright "and related rights."[193] The real difference turns on enforcement. It gives more autonomy to states in their own investigations than does the Budapest Convention and requires less disclosure to and cooperation with other countries.[194] It does, however, have many provisions on cooperation, information sharing, extradition, and related powers.

Crimes against computers are dealt with in articles 289 through 291 of the *Criminal Code* of the Kyrgyz Republic.

Article 289 prohibits unauthorized access to computers and erasing, modifying or copying information. It does not seem to prohibit simple entry to look around. As in Kazakhstan, whose provisions are very similar on all the points, an offence by a group or an insider abusing his or her position is treated more severely.

Article 290 prohibits spreading malware, again in similar terms to Kazakhstan but with higher penalties. Ransomware would be covered by this provision and probably the former one too.

---

[192] For example, some legal systems do not traditionally recognize data as a form of property. Under existing laws, therefore, copying data without authority may not constitute theft, and deleting someone else's data may not constitute damage to property.

[193] Draft United Nations Convention on Cooperation in Combatting Information Crimes. Online:https://www.rusemb.org.uk/fnapr/6394It appears that the UN may have moved (from the original Russian draft) in a slightly more comprehensive direction on cybercrime. The current state of its efforts may be seen online: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home?

[194] A. Peters. 2019. "Russia and China are trying to set the U.N.'s Rules on Cybercrime," Foreign Policy. 16 September. Online: https://foreignpolicy. com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime.

Article 291 is much like 289 with respect to information specially protected by law. Penalties involve being denied access to computers. But the "same action [producing] imprudently grave consequences is punished with imprisonment [for] up to four years."

These days just about everybody understands that fighting cybercrime is exceedingly difficult. Cybercriminals take some pains to disguise their location and tend to attack indirectly. Consumer or user education is a crucial tool for resisting cybercrime. Making the target harder to attack is as important as fighting the attackers.

It would appear that the Kyrgyz Republic's response to cybercrime is adequate in the circumstances. The administration rather than the legislative text will be critical. The multi-year Action Plan on e-commerce mentioned several times in this report gives indirect comfort on this point: it recommends no action on cybercrime among its many suggestions for improvement to national e-commerce laws.

F. Electronic payments

All commerce requires payment, and e-commerce works best with e-payments. For B2C transactions, the world standard is e-payment through credit cards. The card issuer takes the responsibility for identifying and authenticating the card holder and ensures that the merchant is paid (within some contractual limits).

The terms of use are largely set by the large card organizations, notably Visa and Mastercard, subject to the national laws that apply.

The *Law about the Payment System of the Kyrgyz Republic* governs all money in the country, including electronic payment systems.[195] Procedures and requirements about electronic money in the Kyrgyz Republic are established by a resolution of the Board of the National Bank.[196] The resolution applies to domestic banks and to international e-money providers. Banks need a licence to manage e-money.[197]

[195] Law about the Payment System in the Kyrgyz Republic (2015) online: http://cis-legislation.com/document.fwx?rgn=73223.
[196] Resolution of the Board of National Bank about Electronic Money in the Kyrgyz Republic (2016), online: http://cis-legislation.com/document.fwx?rgn=99015.
[197] Footnote 196, article 4.

The resolution goes into substantial detail about how the participants in the e-money system relate to each other and the rules of conduct. E-money can be used only with the consent of the account holder.[198] All e-money in the country must be denominated in the national currency.[199] The resolution provides for the conversion of e-money to traditional currency as well.[200]

However, electronic payments present more difficulties in practice than the legal texts would suggest. Most buyers even of online goods prefer to pay with cash. Even though the Kyrgyz Republic has about three million credit cards outstanding, fewer than 60% of transactions were online, even in Bishkek. The numbers were far lower in rural areas.[201]One challenge to broader use is that bank cards do not allow online payments when issued. The cardholder needs to write an application and apply personally at the bank for permission to trade online. [202]

The multi-year Action Plan (items 10 and 11) wouldundertake to increase the number of services for which one can pay through e-wallets and online banking, but the target date is the fourth quarter of 2026.

The issues with e-payments seem more technical than legal, at this point. To the extent that banks' own procedures impair the use of online transactions, they have the legal ability to relax their precautions.

1. Foreign payments

A separate chapter of a Resolution of the National Bank of the Kyrgyz Republic prescribes rules for international providers of electronic money.[203] "Repayment of the international electronic money can be carried out in foreign or national currency at its sole option the holder of the international electronic money."[204]

Risk management principles and practices are also set out in detail.[205]

[198] Footnote 196, article 60.
[199] Footnote 196, article 7.
[200] Footnote 196, article 56.
[201] Conversation between Iskander Artykbayev and Aikanysh Saparalieva, March 2022.See also the Support Program document, footnote 2, p. 3.
[202] Support Program and e-commerce development in the Kyrgyz Republic for 2022- 2007, footnote 2, p. 3.
[203] Resolution of the Board of National Bank about Electronic Money in the Kyrgyz Republic (2016), footnote 196, articles 69ff.
[204] Footnote 196, article 81.
[205] Footnote 196,chapter 5, articles 85ff

G. Dispute resolution

International best practices
There are internationally recognized legal frameworks for mediation and arbitration, and for the enforcement of arbitral awards. Trading nations are well advised to adopt those frameworks:

- UNCITRAL has a complex array of Mediation texts, described here: https://uncitral.un.org/en/texts/mediation aimed at fair procedure, neutral mediators, and enforceability of the results of the mediation.
- The UNCITRAL Model Law on International Commercial Arbitration sets out the rules for such an arbitration and ensures that the arbitrator can function without undue supervision by national courts of either party. The opportunities for judicial intervention are limited.
- The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards is the international standard for the enforcement of awards. It ensures that awards can be enforced in any of the 100+ member states of the Convention. The Kyrgyz Republic has been a party to this Convention since 1996. It has not adopted the Model Law on international commercial arbitration, or any of the mediation texts.

Legal rights are of little use if they cannot be enforced when needed. Conflicts about the exercise of rights require some means of peaceful resolution. The traditional method of resolving such disputes is the public court system, capable of dealing with civil disputes (mainly between private parties or involving private interests) and criminal disputes (where matters of public order and safety arise.)

However, courts can be expensive, slow and hard for some people to understand. In international disputes, parties may not trust judges in the courts of the adverse party. As a result, less formal alternatives have developed. The main alternative dispute resolution methods are mediation and arbitration.

- Mediation involves a neutral person intervening between or among the disputants, ensuring the continuance of discussion, the generation of options for moving forward,

and the framing of an eventual compromise if the mediation succeeds. The mediator has no power to impose a resolution.

- Arbitration also involves a neutral person hearing the disputants but relies more on resolving their legal rights. The arbitrator has the power to impose a resolution.

Both mediation and arbitration are known in the Kyrgyz Republic. The advantage of either process over the general courts, besides avoiding expense and exposure of the dispute to the public eye, is that the parties may arrange for an expert in the subject-matter of the dispute. In international disputes, mediation and arbitration have the additional advantage that the neutrality of the mediator or arbitrator can be arranged. Disputants do not have to trust the national court system of their adversaries.

It is important to the credibility of the system that settlements resulting from mediation and arbitral awards be enforced, if the parties do not comply with them on their own initiative.For arbitral awards, this is done through the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention"), which has been adopted by some 170 States. It is said, however, that the Kyrgyz Republic expands the list of the grounds for refusal of recognition and enforcement of foreign arbitration awards in comparison with a list of the grounds referred to in the New York Convention. This could have a negative impact on the willingness of foreign parties to enter into transactions with counterparts in the Kyrgyz Republic. [206]

The modern version of alternative dispute resolution is online dispute resolution (ODR). Sometimes ODR just means a regular mediation or arbitration conducted by videoconference over the Internet. More often, however, it can rely on software that leads parties – normally to a mediation – through structured questions and responses, helping to narrow the differences between them – and sometimes ending with an agreement. Designing such systems can be difficult and requires expertise in the subject-matter of the dispute. It can also be difficult to get both sides to potential disputes to agree to participate before any dispute has arisen between them. In some national legal systems, such an agreement (before a dispute arises) would be unenforceable.

[206] US AID, footnote 136, s. 3 Legal regime/dispute resolution.

There is no current plan to introduce ODR to the Kyrgyz Republic. Some international platforms, such as Ali Baba, may offer facilities for resolving disputes among platform participants, as part of the operation of the platform. Such facilities will accustom users to the concept and operation of ODR.

H. Civil liability: private enforcement of good conduct

The law of civil liability helps to compensate people harmed by the faults of others.[207] At the same time it may dissuade people—including businesses and manufacturers—from committing those faults in the first place. The main focus of liability discussions in e-commerce is the potential liability of internet intermediaries, given their potential to create damage but also given their sometimes limited ability to verify information they are called on to transmit.

States designing the civil law framework of a digital economy – including cross-border paperless trade - must therefore examine who will participate in this trade, the relationships between the trading partners (buyers and sellers) and their intermediaries, what can go wrong, and who should bear the risk of this happening (i.e., who is best positioned to avoid the potential harm or best able to take out insurance against it).

This calculation is made more complicated as many participants in a cross-border electronic trade system are public institutions—either government entities, such as customs services, or bodies performing public functions, such as inspection laboratories.

The participants in electronic commerce transactions depend on numerous intermediaries to manage and carry their communications: internet service providers, e-commerce trading platform operators, and trust service providers. For cross-border trade, there are also regulatory authorities, notably the Customs Authority, and possibly a National Single Window to coordinate approvals for their goods and services to cross the border.

However, other policies may complicate the imposition of liability, for example the desire to ensure that the intermediaries continue in business, rather than being crippled by large judgments, and the public agency character of the intermediary (like a single window or the regulatory agencies).
Many countries limit the exposure of taxpayer-funded bodies to substantial money judgments.

[207] This discussion is substantially drawn from the ADB report on e-commerce legislation in CAREC countries, footnote 74.

To date there is little or no experience in the Kyrgyz Republic with civil liability imposed on the intermediaries of e-commerce, either domestic or international. The *Law about e-commerce* of 2021 deals expressly with the liability of intermediaries.[208] For this purpose, "intermediaries" include providers of logistics, communications (notably web hosting, data storage and cloud computing) and financial services to the primary participants in e-commerce, being the seller, buyer and platform operator. Trading platform operators may deserve special attention in this context, given their importance to e-commerce in practice.

The Law provides that an intermediary is not liable for the legality of transmitted or stored electronic messages or goods and services, so long as the intermediary is not the originator of transfer or placement of communications and does not change the content of electronic messages and documents when providing communications services.[209]

These provisions seem satisfactory in principle. We have not heard from traders or others that they are problematic. They are very much in the mainstream of intermediary liability rules around the world.

It is also desirable that any special limitations of liability should be disclosed at the outset, before trading begins, so that potential traders (inside or outside the country) can evaluate their risks. Trading websites or government-sponsored facilities like single window operations are well suited for this kind of disclosure.

Sometimes the limitations can be imposed by contract. E-commerce platform operators would be most likely to attempt such contracts. If the government believes that the resulting contracts are unfair, because they pass on too much risk to the platforms' customers, it may need to legislate a better balance. The fairness calculation should consider that there may be limits on the ability of platform operators to estimate or to avoid the risks arising from those who use the platform. There is no single right answer for every situation.

[208] Footnote 10, article 8(1).
[209] Footnote 10, article 8(2).

However, where the participants can be considered private commercial operations, perhaps subject to competition, then the normal rules of civil liability can be more easily allowed to function.

Civil liability is helpful to bring discipline to a trading system only if recourse to the civil courts is accessible for the parties to disputes. Alternatives to court processes have already been discussed and may also be acceptable forums to determine liability.

VI. RECOMMENDATIONS FOR DEVELOPMENT OF THE LAW

Responding to challenges – overview of policy dynamics210

When weighing the roles of the private sector and state legislative and legal regimes in expanding e-commerce and their contribution to an economy, two issues stand out. The first is the ability of the private sector to conduct e-commerce without further reform. The second is the desirable degree of autonomy for the parties to e-commerce. Both involve assessments of risk and reward and the consideration of two basic questions:

(i) **Is law reform necessary?** In many parts of the world, e-commerce grew before laws were changed. This growth was based on contracts between businesses (trading partner agreements) and on the flexibility of existing laws that allowed novelty. However, there were and are limits to how far private agreements could go to changing basic rules of law. Law reform was more economical of effort and more general of application than contractual regimes. Central Asian countries like the Kyrgyz Republic tended to leave little room for private initiative until the basic laws were enacted to allow for electronic documents and signatures. This study discusses further reforms that go beyond what transacting parties can do for themselves. This section starts with the current law in place and considers building on it.

(ii) **How much regulation or party autonomy should there be?** The degree of regulation required by or wanted in a system greatly depends on the extent of risk the system is willing to tolerate. These risks fall into three broad categories:

[210] This text is largely influenced by sections of the ADB E-Com publication *E-Commerce in CAREC Countries: Laws and Policies*, Footnote 74.

a. ***Risk to the transacting parties themselves.*** **Are the parties able and competent** to make good decisions in novel areas? They may be free to fail, or the state may feel obliged to save them from bad choices. If the latter is the case, then the state is more likely to regulate the choices that lead to the risks. The state may distinguish among parties to "save", protecting consumers more than businesses, for example.
b. ***Risk to others.*** A less regulated system may expose others potentially affected by business-to-business (B2B) or business-to-consumer (B2C) dealings to fraud or mistakes. Some societies are more willing than others to trust the competence and honesty of private actors; others rely on more extensive state oversight of economic activity.
c. ***Risk to public policy****.* Governments differ in how much uncertainty they can tolerate, and in deciding how much business failure should be allowed, and at what cost to the economy. Innovation has benefits and costs.

Risk tolerance differs between parties and states. It is a policy question, not a technical one, and law reform is a form of risk management that reflects this level of tolerance. In part to minimize the need for state regulation, the Kyrgyz Republic may want to support the development of private sector capacities to manage risk.

It may be noted, moreover, that in an economy in transition from a socialist to a market economy, regulation may depend on the desire to control economic activities, mainly in order to implement economic development plans. For instance, the discussion on the mandatory use of national PKI systems is closely related to the desire to control and validate all economic transactions (as it was in socialist law, when contracts were invalid if not foreseen in the economic development plan).

The design of the resulting legislation still depends on policy, though, not on legal principle as such.

A. The statutory framework

The Kyrgyz Republic currently has a collection of statutes affecting electronic commerce, laws about electronic commerce, electronic signature, electronic governance, access to information (several statutes), consumer protection, the protection of privacy, to name only the main ones.

Would it make sense to consolidate them, roll them up into one comprehensive statute on electronic communications?

A good argument can be made that the various statutes do largely have their own distinguishable topics (with the possible exception of some of the access to information laws). It may be easier to find the answers to one's questions in separate statutes than in one very large piece of 'omnibus' legislation. The more important question to ask is consistency: do these laws contradict each other or do they work together well?

In practice, efforts have been made to keep the statutes consistent. When one is amended, others that relate to it have tended to be amended at the same time. The authors of this report have not found any direct inconsistencies among the relevant laws.

It is important when such statutes are being amended that input is sought from all sectors of the economy likely to be affected. Some kind of legislative working group is indicated, with public and private sector participants. Interest groups such as the Electronic Commerce Association should be invited to be at the table. In many cases, financial institutions would need to be part of the discussion, especially since the e-payments system is in need of facilitation.

IT IS RECOMMENDED that the diverse e-commerce statutes now in place should not be consolidated, but that law reform efforts focus on keeping them all co-ordinated when any of them are being amended. A working group on any such amendment should include those principally affected by the proposed amendment, in the public as in the private sector.

B. The Action Plan

The Action Plan of the Cabinet of Ministers for 2023 – 2026[211] contains many good ideas, several of them involving legislative topics, while others involve programs or institutional initiatives. Most but not all of the legislative topics have been mentioned in the course of this report.

IT IS RECOMMENDED that all the legislative items in the Action Plan be carried forward on the timetable set out in that document, subject to what follows.

[211]The Action Plan was open for consultation as a draft for most of 2022. It was finally approved by the Cabinet of Ministers in December 2022 and published in January 2023. Online: http://cbd.minjust.gov.kg/act/view/ru-ru/159827 (The Chrome browser translates the Russian text well.)

1. **Consumer Protection**

The consumer protection proposals of Item 1 are all valuable. Particular attention should be paid to consistency with the relevant rules of the Eurasian Economic Union in this regard.

2. **Privacy**

The personal data protection proposals of Item 2 are also valuable. Some effort is needed to make explanatory material available to data custodians who currently are not certain of their rights or duties in handling personal information. One should ensure that the State Agency responsible for enforcement is capable of doing so at the scale required.

3. Data Localization

Some caution is needed, however, in that Item's "mandatory placement and storage of personal data of citizens of the Kyrgyz Republic in the territory of the Kyrgyz Republic." The political appeal of such a measure is clear, but the measure may have an expensive effect on the operations of cross-border businesses who would need semi-independent or firewalled data centers in many countries. As noted in the report, free trade agreements often prohibit such measures. It may be prudent for the Kyrgyz Republic to delay implementing this measure until it joins the ESCAP Framework Agreement (as recommended below) and can discuss the merits with that body's technical and legal advisory groups. The OECD has several studies on the topic.[212]

4. **Valuation of digital trade**

Joining the comprehensive framework of the OECD project on valuation of digital trade and the impact on taxation, as set out in Action Plan Item 3, is a good idea. Cross-border collaboration is essential to ensure honest reporting of valuations that affect the revenues of many states.

(That item refers to accession to the UN Convention on Contracts for the International Sale of Goods. According to the United Nations, which is the depositary of the treaty, the Kyrgyz Republic is already a member state of that Convention.)

[212] OECD, "A Preliminary Mapping of Data Location Measures", June 2022, online: https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en AND "Data localisation trends and challenges" (December 2020), online: https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en

5. **Remote signature and authentication**

The draft version of the Action Plan proposed reforms to electronic signature law to expand the opportunities for remote identification and authentication are a topic of current interest in many places around the world.[213] Remote signature was a pressing need during the covid pandemic and still has its advocates. Many such initiatives rely on real-time video connections and readily available digital signatures to make such systems work. Consideration would be needed whether the technological infrastructure is available in the Kyrgyz Republic to support such a legal underpinning to remote signing systems. This item does not appear in the final version of the Action Plan but is nonetheless worth considering.

6. **Electronic certificates of origin**

Electronic certificates of origin as contemplated by Action Plan Item 7 are very valuable and would save cost and effort, notably in a single window system. Normally their use depends on agreement with trading partners to accept them and produce them according to accepted rules.

7. **National single window**

It makes sense to have a legislative framework for a national single window, as mentioned in Action Plan Item 8 – now under the name of One Stop Shop - and not just a network of contracts among participants – though contractual undertakings of service levels to be maintained can be a useful supplement to the legislation. CEFACT has practical and legal standards that are referred to below in item 14 of this list.

8. **Electronic payments**

Upgrading the e-payments system and practices, as Action Plan Items 10 and11 suggest, will be very helpful. Much of the upgrade will not depend on legislation, but some of the permissions required will no doubt benefit from legislative reinforcement. Input should be sought from the banking and financial technology sectors.

9. **Tax incentives**

[213] The Submission of the E-Commerce Association of the Kyrgyz Republic to the ADB, July 2002, paragraph 6, supported these goals. The Association supported almost all of the Ministry's Action Plan.

Many countries encourage electronic commerce through tax policies. It is beyond the scope of this report to design tax policy for the Kyrgyz Republic. It can be noted that the Electronic Commerce Association had comments on how the tax system should be designed for the purpose. In addition, the exemption from customs duties for packages of small value ("de minimis") can facilitate cross-border trade in useful ways.

C. International issues

A constant theme of any writing on law and e-commerce is the desirability of harmonizing one's laws with that of one's neighbors and trading partners. Electronic trade flows naturally across borders with electrical and communications systems, and the more the law on both sides of the border is compatible, the easier it is for traders to participate. This report has mentioned a number of possible international instruments in which the Kyrgyz Republic could be engaged.

IT IS RECOMMENDED that the Kyrgyz Republic accede to or adopt the following instruments, in descending order of their desirability or importance.[214]

10. ESCAP Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific.

The Framework Agreement promotes a high common standard for paperless trade law and also offers facilities for exchange of expertise and some financial assistance in complying with its term. One could refer to the report done for the Ministry of the Economy and Trade by the International Trade Centre on the country's readiness for cross-border paperless trade.[215]

11. WTO Trade Facilitation Agreement

Continue implementing the TFA under the schedule currently accepted by the WTO.

12. UN Convention on the Use of Electronic Communications in International Contracts

The ECC helps standardize the law already largely compatible with Kyrgyz statutes – the UNCITRAL Model Laws – and also gives the opportunity to interpret other treaties

[214] More information and links to online documents and explanations appear in the International section IV of this report.
[215] A draft of this report was mentioned at footnote 149.

consistently with them. It can also be used as the basis for domestic law, though there may be little need for that at this stage for the Kyrgyz Republic.

13. UN Harmonization of Frontier Controls and Layout Rules

Creating and recognizing documents in these standard forms may remove the need for translation of many of them and makes compliance with foreign expectations much easier, as well as making foreign documents more recognizable in the Kyrgyz Republic.

14. UNE/CEFACT Recommendations for the National Single Window

When legislating to create the National Single Window (or “one stop shop” facility), close attention should be paid to the CEFACT standards, which have created expectations among international traders.

15. UNCITRAL Model Law on Electronic Transferable Records

As traders become ready to accept electronic versions of bills of lading, warehouse receipts and the like, Kyrgyz law should recognize the standards of reliability set out in this Model Law. This Model Law is gradually being adopted around the world. Advice may be taken from the principal trading partners as to timing.

16. International Standards Organization

Expert advice should be sought on how and when to impose the ISO’s Series 27000 standards on technological operations in the Kyrgyz Republic. They are the international state of the art.

17. **Convention on the Recognition and Enforcement of Foreign Arbitral Awards** [Not accession but better conformity to required practices]

The Kyrgyz Republic should conform closely to the rules of the New York Convention in its treatment of foreign arbitral awards. In this way it can remain a credible partner in international arbitration if a Kyrgyz party needs to have recourse to such a procedure. Being cited in U.S. State Department publications as an unreliable partner in such arbitrations will not serve Kyrgyz business interests well. There may be strong public policy reasons for the positions taken so far, and they may continue to prevail. This recommendation is limited to urging careful consideration of the balance of policies.

18. Regional Comprehensive Economic Partnership (RCEP)

Consider whether the Republic's trading partners are joining RCEP; if so, accede as well to maintain the advantages of free trade. The e-commerce provisions of RCEP are largely compatible with current Kyrgyz law and with the standards of the ESCAP Framework Agreement mentioned earlier.

19. UNCITRAL Model Law on Identity Management and Trust Services (2022)

Verify that Kyrgyz law is consistent with this Model Law in its treatment of trust services, to the extent that Kyrgyzstan is interested in exchanging identity credentials and trusted data with EU member States.

D. Other law reform

Several other areas of prospective reform have been mentioned in the report and deserve follow-up here for the sake of completeness.

IT IS RECOMMENDED that legislation be introduced for the following purposes:

1. Data protection

The Kyrgyz Republic should legislate more clearly to actively protect the confidentiality of any data – commercial or personal – that is not in its usual state accessible to the public. This could build on the current protection for trade secrets and related commercial information, the source of which is harder to locate than it should be. Such legislation could be similar to the *Law on Personal Information.* It should prohibit the collection, use or disclosure of commercial or other confidential information except by express consent of the owners.

2. Whistleblower protection

Consider adding whistleblower protection to one of the laws on access to information. There may be some resistance to such legislation, as whistleblowers are not always popular with their colleagues or management. They rock the boat, but in the public interest. Prior screening may be useful, by which some neutral party evaluates the importance of the public interest compared to the harm done to the organization whose activity is to be exposed for public scrutiny. Models of whistleblower laws are available when the work is undertaken.

CONCLUSIONS

The Kyrgyz Republic has done some constructive and imaginative law reform on electronic commerce over the past years. Its current collection of statutes holds up well on analysis for domestic purposes and also in comparison to its major trading partners.

Many countries have similar agendas in these pandemic or post-pandemic times, to support online trade and the ability of their residents and businesses – and regulators – to participate in it.

Thus harmonization is a top priority. It is important to build linkages both formal and informal to bodies with a harmonizing agenda.

This report has examined Kyrgyz law in the light of international standards and has considered the opportunities to advance harmonization. Its marks are quite good, and where paperless trade – domestic and cross-border – is not happening, the cause is often not deficiencies in legislation or regulation but in technology and culture, and in financial resources to take advantage of the opportunities that do exist.

Our competence and our mandate have, however, been limited to legislation and regulation. In our view, following the recommendations in the last section of the report will help the Kyrgyz Republic advance its digital economy agenda in step with its neighbours and trading partners. We hope that the results will justify our optimism.

THE END

THE END