**End-to-end trade digitalization: Questionnaire on regulatory analysis – South Africa**

**Introduction**

The United Nations Commission on International Trade Law (UNCITRAL) at its fifty-seventh session requested the secretariat to conduct a stocktaking exercise to examine all UNCITRAL legislative texts that referred to electronic aspects, including both UNCITRAL texts on electronic commerce and other texts that include provisions on the use of electronic means (A/79/17, para. 299). The Commission also requested a survey of the enactment of those texts and of the references to such texts contained in trade agreements. The secretariat was requested to circulate a questionnaire inviting States to provide the information and to submit copies of the relevant laws.

This Questionnaire has been prepared by the International and Comparative Law Research Center (ICLRC) as a part of its research complementing the stocktaking exercise of the secretariat and is aimed at harmonizing the existing approaches to digital trade. The main objectives of the ICLRC research are to identify the current state of implementation of the UNCITRAL documents, as well as to outline the alternative approaches and possible gaps.

This Questionnaire embraces [MLEC](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf), [MLES](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf), [ECC](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf), [MLETR](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf), [MLIT](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_en.pdf), [MLAC](https://uncitral.un.org/sites/uncitral.un.org/files/mlac_en.pdf). It consolidates the UNCITRAL’s provisions on end-to-end trade digitalization based on the existing model laws and the convention in a generalized form in order to avoid duplication.

**Instructions**

This Questionnaire consists of seven parts. The first part deals with the regulatory landscape of your country. Kindly check which areas of digital trade are already covered by specific laws and briefly describe how each of the UNCITRAL General Principles is implemented in your country.

Parts II to VI are based on the relevant model laws and the convention. When answering the questions, please use one of the three colours to fill in the cells in accordance with the colour coding of the study:

|  |  |  |
| --- | --- | --- |
| **no regulation:**  the subject matter is not subject to any specific regulation in your country, but general rules of commercial or contract law may apply | **UNCITRAL regulation:**  the relevant UNCITRAL provision is fully incorporated in the laws of your country. We kindly ask you to briefly describe this regulation | **alternative regulation:** the issue addressed by the relevant UNCITRAL provision is regulated in the alternative manner by the laws of your country. We kindly ask you to briefly describe your country's approach so that we can use it for the proposals for further harmonization and consolidation of UNCITRAL instruments. |

Part VII deals with the regulatory gaps and aims at identifying the areas not yet covered by the UNCITRAL instruments.

The ICLRC would appreciate receiving responses by the end of February to allow time for compilation and analysis. The ICLRC reserves the right to make the information you provide publicly available unless you indicate otherwise.

**Part I. General**

What special laws are there in your country?

☒on electronic commerce/digital trade

|  |
| --- |
| 2002 Electronic Communications and Transactions Act (ECTA) |

☒on electronic/digital signatures

|  |
| --- |
| 2002 Electronic Communications and Transactions Act (ECTA) |

☒on identity and trust services

|  |
| --- |
| 2013 Protection of Personal Information Act (POPIA), 1993 Trade Marks Act, 1978 Copyright Act, 1978 Patents Act, 2008 Consumer Protection Act (CPA) |

☐on automated contracting

|  |
| --- |
|  |

☐on electronic/digital transferrable records

|  |
| --- |
|  |

**Adherence to the UNCITRAL General Principles**

|  |  |  |
| --- | --- | --- |
| **UNCITRAL principle** | **Content of provision** | **Implementation in your country** |
| Non-discrimination | Non-discrimination between information on a paper medium and information communicated or stored electronically. | For e-signatures, statements and documents if certified |
| Technology neutrality | No discrimination should be made among the various techniques that may be used to communicate or store information electronically. | Yes, the promotion of technology neutrality in the application of legislation to electronic communications and  transactions is stated in the national law |
| Functional equivalence | Analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. | For e-signatures, statements and documents if certified |

**Part II. Electronic communications**

no regulation,UNCITRAL regulation**,** alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Consent to use | Nothing requires a party to use or accept electronic communications, but a party’s agreement to do so may be inferred from the party’s conduct. | An acknowledgement of receipt of a data message is not necessary to give legal effect to that message. (2) An acknowledgement of receipt may be given by—(a) any communication by the addressee, whether automated or otherwise; or (b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.  Source: Electronic Communications and Transactions Act 2002 (upd. 2021), article 26 |
| Technological neutrality of communication | The rules do not depend on or presuppose the use of particular types of technology and could be applied to communication and storage of all types of information. | Implemented  Source: ECTA 2002 (upd. 2021), article 2 |
| Writing | The requirement to be in writing is met if the information is accessible so as to be usable for subsequent reference. | Implemented  Source: ECTA 2002 (upd. 2021), article 12 |
| Original | Requirement to be in original is met if the integrity of the information is assured from the time when it was first generated in its final form and, where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available. | Implemented  Source: ECTA 2002 (upd. 2021), article 14 |
| Time of dispatch | The time of dispatch of an electronic communication is the time when it leaves an information system or, if the electronic communication has not left an information system, the time when the electronic communication is received. | Implemented  Source: ECTA 2002 (upd. 2021), article 23 |
| Time of receipt | The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. | Implemented  Source: ECTA 2002 (upd. 2021), article 23 |
| Place of dispatch and receipt | An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business. | Implemented  Source: ECTA 2002 (upd. 2021), article 23 |
| Invitations to make offers | Advertisement is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance. | The publication of an advertisement offering goods for sale at a stated price is not an offer to all who may read the advertisement but merely an invitation to make offers: Bird v Summerville 1960 4 SA 395(N) 401D. This is referred to as an invitation to treat. |
| Withdrawal due to error | The party that made the error has the right to withdraw the portion of the electronic communication in which the input error was made if:  (a) other party was notified of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and  (b) the party that made the error has not used or received any material benefit or value from the goods or services, if any, received from the other party. | Implemented |

**Part III. Electronic signatures**

no regulation,UNCITRAL regulation,alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Signature technology neutrality | The law recognizes any method of creating an electronic signature that satisfies the requirements. | Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.  Source:Electronic Communications and Transactions Act 2002 (upd. 2021), article 13 |
| Compliance with a requirement for a signature | Where the law requires a signature of a person (either in the form of an obligation or in the form of consequences for the absence of a signature), that requirement is met if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated. | Implemented  Source:Electronic Communications and Transactions Act 2002 (upd. 2021), article 13 |
| Reliability of signature | An electronic signature is considered to be reliable if:  (a) The signature creation data are linked to the signatory and to no other person;  (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;  (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and  (d) 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, any alteration made to that information after the time of signing is detectable. | Where an electronic signature is required by the parties to an electronic transaction and the parties  have not agreed on the type of electronic signature to be used, that requirement is met in relation to a  data message if-  (a) a method is used to identify the person and to indicate the person's approval of the information  communicated; and  (b) having regard to all the relevant circumstances at the time the method was used, the method  was as reliable as was appropriate for the purposes for which the information was communicated Source:Electronic Communications and Transactions Act 2002 (upd. 2021), article 13 |
| Conduct of the signatory | Signatory shall:  (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;  (b) Without undue delay, notify that the signature creation data have been compromised; or there is a substantial risk that the signature creation data may have been compromised;  (c) Ensure the accuracy and completeness of all material representations that are included in the certificate;  (d) Bear the legal consequences of its failure to satisfy the above mentioned requirements. | No regulation |
| Conduct of the certification service provider | Certification service provider shall:  (a) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate or that are included in the certificate;  (b) Provide reasonably accessible means that enable a relying party to identify the certification service provider, verify the signatory and its control of the signature creation data at the time when the certificate was issued; and to verify that signature creation data were valid at or before the time when the certificate was issued;  (c) Provide reasonably accessible means that enable a relying party to ascertain:  (i) The method used to identify the signatory;  (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;  (iii) That the signature creation data are valid and have not been compromised;  (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;  (v) Whether means exist for the signatory to give notice that the signature creation data have been compromised;  (vi) Whether a timely revocation service is offered;  (d) Bear the legal consequences of its failure to satisfy the above mentioned requirements. | Implemented (but is called “Accreditation authority”)  Source: ECTA 2002 (upd. 2021), article 36 |
| Requirements to certification service providers | In determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:  (a) Financial and human resources, including existence of assets;  (b) Quality of hardware and software systems;  (c) Procedures for processing of certificates and applications for certificates and retention of records;  (d) Availability of information to signatories identified in certificates and to potential relying parties;  (e) Regularity and extent of audit by an independent body;  (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing;  (g) Any other relevant factor. | Implemented  Source: ECTA 2002 (upd. 2021), article 38 |
| Conduct of the relying party | A relying party shall bear the legal consequences of its failure:  (a) To take reasonable steps to verify the reliability of an electronic signature; or  (b) Where an electronic signature is supported by a certificate, to take reasonable steps:  (i) To verify the validity, suspension or revocation of the certificate; and  (ii) To observe any limitation with respect to the certificate. | No regulation |
| Recognition of foreign certificates and electronic signatures | A certificate issued or an electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate (or signature) issued (created or used) in [the enacting State] if it offers a substantially equivalent level of reliability.  In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability, regard shall be had to recognized international standards and to any other relevant factors. Where parties agree to use certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law. | (1) The Minister may, by notice in the Gazette and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.  (2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1) is guilty of an offence.  Source: ECTA 2002 (upd. 2021), article 40 |

**Part IV. Identity and trust services**

no regulation,UNCITRAL regulation, alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| E-identification and identity proofing | Where the law requires the identification of a person, or provides consequences for the absence of identification, that requirement is met with respect to identity management services if a reliable method is used for the identity proofing and electronic identification. | Implemented |
| Electronic seals | Where the law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement is met if a reliable method is used:  (a) To provide reliable assurance of the origin of the data message; and  (b) To detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display. | Where a seal is required by law to be affixed to a document and such law does not prescribe the  method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic  signature of the person by whom it is required to be sealed Source: ECTA 2002 (upd. 2021), article 19 |
| Electronic timestamps | Where the law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement is met if a reliable method is used:  (a) To indicate the time and date, including by reference to the time zone; and  (b) To associate that time and date with the data message. | No regulation |
| Electronic archiving | Where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met if a reliable method is used:  (a) To make the information contained in the data message accessible so as to be usable for subsequent reference;  (b) To indicate the time and date of archiving and associate that time and date with the data message;  (c) To retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and  (d) To retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received. | Implemented |
| Electronic registered delivery services | Where the law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement is met if a reliable method is used:  (a) To indicate the time and date when the data message was received for delivery and the time and date when it was delivered;  (b) To detect any alteration to the data message after the time and date when the data message was received for delivery to the time and date when it was delivered, apart from the addition of any endorsement or information required by this article, and any change that arises in the normal course of communication, storage and display; and  (c) To identify the sender and the recipient. | No regulation |
| Website authentication | Where the law requires website authentication, or provides consequences for the absence of website authentication, that requirement is met if a reliable method is used:  (a) To identify the person who holds the domain name for the website; and  (b) To associate that person to the website. | No regulation |
| Ex post recognition of reliability | The method shall be deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the designated function, by itself or together with further evidence.  In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include compliance with the legal requirements or any applicable recognized international standards and procedures relevant for the provision of the service, as well as any supervision or certification provided with regard to the service. | Implemented  Source: ECTA 2002 (upd. 2021), article 13(3) |
| Ex ante designation | A [person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent] may designate identity management or trust services that are presumed reliable. | Implemented  (Accreditation of authentication service providers) |
| Obligations in case of data breach | If a breach of security or loss of integrity occurs that has a significant impact on a service, the service provider shall, in accordance with the law:  (a) Take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;  (b) Remedy the breach or loss; and  (c) Notify the breach or loss. | No regulation |
| Cross-border recognition | The result deriving from the use of an identity management or trust service provided outside [the enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as the result deriving from the use of an identity management or trust service provided in [the enacting jurisdiction] if the method used by the service offers:  (a) At least an equivalent level of reliability, where the reliability levels recognized by such jurisdictions are identical; or  (b) Substantially equivalent or higher level of reliability, in all other cases.  For the purposes of determining the reliability level regard shall be had to recognized international standards. The identity management or trust service shall be presumed to be reliable if [the person, organ or authority specified by the enacting jurisdiction] has ex ante determined the equivalence. | (1) The Minister may, by notice in the Gazette and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.  (2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1) is guilty of an offence.  Source: ECTA 2002 (upd. 2021), article 40 |

**Part V. Automated contracting**

no regulation,UNCITRAL regulation,alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Legal recognition of automated contracting | A contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in any action carried out in connection with the formation of the contract  An action carried out by an automated system in connection with the formation or performance of a contract shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed or intervened in the action. | Different regulation for natural and legal persons  Source: ECTA 2002 (upd. 2021), article 20 |
| Computer code and dynamic information | A contract shall not be denied validity or enforceability on the sole ground that the terms of the contract are contained in data messages in the form of computer code.  A contract or an action in connection with it shall not be denied validity or enforceability on the sole ground that it is based on information from a data source that provides information that changes periodically or continuously. | No regulation |
| Attribution of actions carried out by automated systems | As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties. If this does not apply, an action carried out by an automated system is attributed to the person who uses the system for that purpose. | A data message is that of the originator if it was sent by—  (a) the originator personally;  (b) a person who had authority to act on behalf of the originator in respect of that data message; or  (c) an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming. |
| Unexpected actions carried out by automated systems | Unless otherwise agreed by the parties, where an action carried out by an automated system is attributed to a party to a contract, the other party to the contract is not entitled to rely on that action if:  (a) The party to which the action is attributed could not reasonably have expected the action; and  (b) The other party knew or could reasonably be expected to have known that the party to which the action is attributed did not expect the action. | No regulation |
| Non-avoidance | Unless otherwise provided by law, a party shall not be relieved from the legal consequences of its failure to comply with a rule of law on the sole ground that it used an automated system. | No regulation |

**Part VI. Electronic transferrable records**

no regulation,UNCITRAL regulation,alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Transferable documents or instruments | Where the law requires a transferable document or instrument, that requirement is met by an electronic record if:  (a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and  (b) A reliable method is used:  (i) To identify that electronic record as the electronic transferable record;  (ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and  (iii) To retain the integrity of that electronic record. | Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if - Page 21 of 62 Prepared by: In partnership with: (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and (b) that information is capable of being displayed or produced to the person to whom it is to be presented. (2) For the purposes of subsection 1(a), the integrity must be assessed- (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;  Source: ECTA 2002 (upd. 2021), article 13 |
| Control | Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:  (a) To establish exclusive control of that electronic transferable record by a person; and  (b) To identify that person as the person in control. | No regulation |
| Transfer | Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record. | No regulation |
| Endorsement | Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements. | the integrity must be assessed- (a) by considering whether the information has remained complete and Unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display  Source: ECTA 2002 (upd. 2021), article 13 |
| Amendment | Where the law requires or permits the amendment of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used for amendment of information in the electronic transferable record so that the amended information is identified as such. | No regulation |

**Part VII. Other issues**

Please identify the three most important issues related to the electronic commerce or digital trade that are not covered by UNCITRAL documents, but are or will be regulated in your country:

1. Data Localization and Cross-Border Data Flows

While UNCITRAL has guidelines on electronic contracts and dispute resolution, it doesn't focus deeply on privacy laws or data protection in e-commerce. In South Africa, POPIA regulates how personal data should be handled by businesses in the digital space, including online transactions, data collection, processing, and storage. This law ensures that individuals' personal information is protected from misuse, which is increasingly crucial in e-commerce and digital trade.

While POPIA does not explicitly mandate data localization, it imposes strict conditions on cross-border data transfers, effectively encouraging local storage. This contrasts with UNCITRAL's more neutral stance on data localization, which generally promotes free flow of data across borders.

2. Digital Taxation and E-Commerce Transactions

UNCITRAL documents do not specifically address digital taxation, leaving it to individual countries to regulate. South Africa has introduced a digital services tax and expanded its value-added tax (VAT) regime to include digital products and services. For example, foreign e-commerce companies selling digital services to South African consumers are required to register for VAT in South Africa.

3. Consumer Protection in E-Commerce (Focus on Vulnerable Populations)

The Consumer Protection Act (CPA) of 2008 has been adapted to address e-commerce transactions, including provisions for cooling-off periods, disclosure requirements, and dispute resolution. Additionally, South Africa is exploring further regulations to protect vulnerable consumers in the digital economy, populations with limited digital literacy or access to technology. Issues such as online fraud, misleading advertising, and unfair contract terms are prevalent. The Cybercrimes Act (2020) establishes offenses related to cybercrimes, including identity theft, hacking, and the unauthorized interception of data, which are crucial aspects of digital commerce. While UNCITRAL deals with issues like contract formation and dispute resolution, it does not specifically address the complex cybersecurity risks and fraud challenges arising from digital trade.