National Digital Economy and E-Governance Act, 2024

JULY, 2024

Arrangement of Sections

A Bill for an Act to enable the growth of Digital Economy and digital governance in Nigeria by improving the certainty of digital transactions, digital service delivery, and matters related.

CHAPTER ONE - OBJECTIVES, SCOPE AND APPLICATION

1. Objectives

a. To enhance the use of digital technology to grow Nigeria's economy.

b. To create an enabling environment for fair competition to promote innovation, growth, and competitiveness for the Nigerian Digital Economy.

c. To create export-oriented capacities in Nigeria's digital economy to improve Nigeria's balance of trade and services.

d. To mandate, promote and enable the digital transformation of public institutions and Government processes for efficient and effective service delivery.

e. To encourage and improve service delivery, openness and accountability for delivery of public or citizen digital services.

f. To provide a legal framework to support international digital trade and investments using digital means.

g. To create a framework for the enhancement of digital economy governance amongst the Ministries, Departments and Agencies.

2. Scope and Application

Applies to all public service institutions, private establishments, individuals and organisations conducting digital activities in Nigeria, either wholly or in part.

CHAPTER TWO - ELECTRONIC TRANSACTION

PART I– VALIDITY OF ELECTRONIC TRANSACTION

1. Requirements for Legal Recognition

An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is rendered or made available in electronic form.

2. Requirement to provide information in writing

(1) Where any information is required by any law to be in writing, recorded in writing or in printed form, or is described as written, notwithstanding anything contained in the law, the requirement or description, shall be satisfied if the information or matter is–

(a) rendered, recorded, or made available in electronic form, accessible to, and is capable of retention by the intended recipient to be usable or retrievable for a subsequent reference.

(2) Sub-section (1) shall apply whether the requirement for the information to be, in writing or recorded in writing, is in the form of an obligation or the law provides consequences if it is not in writing.

(3) Where sub-section (1) applies, a legal requirement to provide multiple copies of any information or other matter to the same person at the same time is met by providing a single electronic form of the information or other matter.

(4) Where any information is retained in electronic form in accordance with sub-section (1) and is retrievable at any time during the specified period of retention, the paper or other non-electronic form of that information need not be retained.

3. Requirement to provide access to information in paper form.

A legal requirement to provide access to information that is in paper or other non-electronic form, is satisfied by providing access to the information in electronic form where the form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose and circumstances in which, access to the information is required to be provided.

4. Delivery of information

(1) Where information is required by law to be delivered, dispatched, given, sent, or be served on a person, the requirement is met by doing so in the form of an electronic record.

(2) Sub-section (1) applies whether the requirement for delivery, dispatch, giving, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, given, sent or served.

5. Information in original form

(1) Where information is required by law to be presented or retained in its original form, the requirement is met by an electronic communication if the integrity of the information can be determined in its final form as an electronic communication or otherwise.

(2) Sub-section (1) shall apply whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of sub-section (1)

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the additions of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required is to be assessed in light of the purpose for which the information was generated and all the relevant circumstances.

6. Retention of documents, records or information in electronic form

(1) Where certain documents, records or information are required by law to be retained in paper or other non-electronic form, that requirement is met by retaining it in electronic form if the following conditions are satisfied–

(a) the information contained in electronic form is accessible to be usable for subsequent reference;

(b) the electronic communication is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) any information that enables the identification of the origin and destination of an electronic communication and the date and time when it was sent or received, is retained.

(2) An obligation to retain documents, records or information in accordance with sub-section (1)(c) shall not apply to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement under sub-section (1) by using the services of any other person, if the conditions set out in sub-section (1) are met.

(4) Nothing in this section shall preclude any public institution from specifying additional requirements for the retention of electronic communications that are subject to the powers and function of the public institution.

7. Other Requirements

(1) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print", "register" or words or expressions of similar effect, shall be interpreted to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

(2) Where a seal is required by any law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed, that requirement shall be met if the electronic document indicates that–

(a) it is required to be under seal and includes the digital signature of the person by whom it is required to be sealed; or

(b) it is required to be under seal and another type of electronic seal is used.

(3) Where information, a signature, document or record is required by any law by contract or deed to be notarised, apostilled, acknowledged, verified or made under oath, the requirement shall be satisfied if, in relation to an electronic signature, electronic document or electronic record, the electronic signature of the person authorised to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the electronic signature, electronic document or electronic record.

(4) Where the law requires payment to be made or issuance of any receipt of payment, that requirement shall be met if payment is made, or receipt is issued by an electronic means in accordance with legislations relating to electronic transactions.

8. Comparison of documents with original

A legal requirement to compare a document with an original may be satisfied by comparing that document with an electronic form of the original document, if the electronic form reliably assures the maintenance of the integrity of the document.

9. Admissibility of electronic records

In proceedings in a court, tribunal or arbitration, whether of a legal, judicial, quasi-judicial or administrative nature, the admissibility of an electronic record or an electronic signature in evidence shall not be denied on the grounds that it is an electronic record or an electronic signature.

PART II – ELECTRONIC CONTRACTS

10. Formation and validity of contracts

(1) For the avoidance of doubt, in the context of the formation of contracts, an offer and acceptance may be given by means of electronic communications.

(2) Where an electronic communication is used in the formation of a contract, that contract shall not be denied validity or enforceability on the ground that an electronic communication was used for that purpose.

11. Validity of Declaration of Intent in Electronic Communications

As between the originator and the addressee of an electronic communication, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability on the ground that it is in the form of an electronic communication.

12. Time and place of dispatch and receipt of electronic communications

(1) The time of dispatch of an electronic communication is–

(a) the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator; or

(b) if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time is when the electronic communication is received.

(2) The time of receipt of an electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

(3) The time of receipt of an electronic communication at an electronic address that has not been designated by the addressee is the time when the electronic communication becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

(4) For the purposes of sub-section (3), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

(5) 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.

(6) Sub-sections (2), (3) and (4) shall apply not withstanding that the place where the information system supporting an electronic address is located, is different from the place where the electronic communication is deemed to be received under sub-section (5).

13. Invitation to make offer or treat

A proposal to conclude a contract, made through one or more electronic communications, which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including a proposal that uses interactive applications for the placement of orders through the information systems, shall be considered as an invitation to make offers or treat, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

14. Use of automated message systems for contract formation

A contract formed by the interaction of an automated system and an individual, or by the interaction of automated systems, shall not be denied validity or enforceability on the ground that no individual reviewed or intervened in each of the individual actions carried out by the automated systems or the resulting contract.

15. Error in electronic communications.

(1) Where an individual makes an input error in an electronic communication exchanged with the automated system of another party and the automated system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.

(2) Sub-section (1) shall not apply unless the person, or the party on whose behalf that person was acting–

(a) notifies the other party of the error as soon as reasonably practicable, after having learned of the error and indicates that he made an error in the electronic communication; and

(b) has not used or received any material benefit or value from the goods or services received, if any, from the other party.

(3) Nothing in this section shall affect the application of any law that may govern the consequences of any error other than as provided for in sub-sections (1) and (2).

PART III – ELECTRONIC SIGNATURES

16. Requirement for signature

Where a law requires a signature or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record.

17. Digital signature

(1) Where, through the application of a specified security or commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made–

(a) unique to the person using it;

(b) capable of identifying the person using it;

(c) created in a manner or using a means under the sole control of the person using it;

(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated; and

(e) where the 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, such signature shall be treated as digital signature.

18. Presumptions relating to digital records and signatures

(1) In any proceedings involving a digital signature, it shall be presumed, unless evidence to the contrary is adduced, that–

(a) the digital signature is the signature of the person to whom it correlates; and

(b) the digital signature was affixed by that person with the intention of signing or approving the electronic record.

19. Equal treatment of signatures

Unless otherwise provided by law, the parties to an electronic transaction may agree to the use of a particular method or form of electronic signature or security procedure.

20. Recognition of foreign certificates and electronic signatures

(1) In determining the extent to which a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business.

(2) Where the parties to a transaction agree to the use of a type of electronic signature and certificates, that agreement shall be sufficient for the purpose of cross border recognition in respect of that transaction.

21. Recognition of foreign certificates and electronic signatures

(1) Where signature creation data or authentication data can be used to create a signature or authenticate any electronic record that has legal effect, each signatory shall–

(a) exercise reasonable care to avoid unauthorised use of its signature creation data or authentication data; and

(b) without undue delay, notify any person who may reasonably be expected by the signatory to rely on or provide services in support of the electronic signature if–

(i) the signatory knows that the signature creation data or authentication data has been compromised.

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data or authentication data may have been compromised; or

(iii) where a certificate is used to support the electronic signature or authentication data, exercise reasonable care to ensure the accuracy and completeness of all material representation made by the signatory, which are relevant to the certificate throughout its lifecycle, or which are to be included in the certificate.

PART IV – ELECTRONIC TIME STAMPS

22. Legal effect of electronic time stamps

(1) An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings on the grounds that it is in an electronic form or that it does not meet the requirements set out in Section 27 of this Act.

(2) An electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

23. Requirements for electronic time stamps

(1) An electronic time stamp shall meet the following requirements–

(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably.

(b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using a digital signature, or by some equivalent method.

(2) Compliance with the requirements laid down in regulations made under sub-section (1) shall be presumed where the binding of date and time to data and the accurate time source meets those standards.

PART V – ELECTRONIC TRANSFERABLE RECORDS

24. Application of this Part

Other than as provided for in this Act, nothing in this Part affects the application to an electronic transferable record of any rule of law governing a transferable document or instrument, including any law applicable to consumer protection.

25. Additional information in electronic transferable records

Nothing in this Act precludes the inclusion of information in an electronic transferable record in addition to that contained in a transferable document or instrument.

26. General reliability standard

(1) For the purposes of this Part, a method shall be deemed reliable if it is–

(a) as reliable as is appropriate for the fulfilment of the function for which the method is being used in light of all relevant circumstances, including–

(i) any operational rules relevant to the assessment of reliability;

(ii) the assurance of data integrity;

(iii) the ability to prevent unauthorized access to and use of the system;

(iv) the security of hardware and software;

(v) the regularity and extent of audit by an independent body;

(vi) the existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method; or

(vii) any applicable industry standard; or

(b) proven in fact to have fulfilled the function by itself or together with further evidence.

27. Legal requirement for transferable documents or instruments

(1) A law that requires a transferable document or instrument is met by a data message if–

(a) the data message contains the information that would be required to be contained in a transferable document or instrument; and

(b) a reliable method is used to–

(i) identify that data message as the electronic transferable record;

(ii) render that data message capable of being subject to control from its creation until it ceases to have any effect or validity; and

(iii) retain the integrity of that data message.

(2) For the purposes of sub-section (1)(b)*(iii)*, the criterion for assessing integrity shall be whether information contained in the electronic transferable record, including any authorized change that arises from its creation until it ceases to have any effect or validity, has remained complete and unaltered apart from any change which arises in the normal course of communication, storage and display.

28. Control.

(1) Any law that requires or permits the possession of a transferable document or instrument is met with respect to an electronic transferable record if a reliable method is used to

(a) establish exclusive control of that electronic transferable record by a person; and

(b) identify that person as the person in control.

(2) A law that requires or permits transfer of possession of a transferable document or instrument is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

29. Indication of time and place in electronic transferable record

Where a law requires or permits the indication of time or place with respect to a transferable document or instrument, such requirement is met if a reliable method is used to indicate that time or place with respect to an electronic transferable record.

30. Endorsement

Where a law requires or permits the endorsement in any form of a transferable document or instrument, such a 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 set forth in Sections 6 and 20.

31. Amendment

Where a law requires or permits the amendment of a transferable document or instrument, such 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.

32. Replacement of an electronic transferable record with a transferable document or instrument

(1) An electronic transferable record may replace a transferable document or instrument if a reliable method for the change of medium is used.

(2) For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the electronic transferable record.

(3) Upon issuance of the electronic transferable record in accordance with this section, the transferable document or instrument shall be made inoperative and ceases to have any effect or validity.

(4) A change of medium in accordance with this section shall not affect the rights and obligations of the parties.

33. Replacement of a transferable document or instrument with an electronic transferable record

(1) A transferable document or instrument may replace an electronic transferable record if–

(a) a reliable method for the change of medium is used; and

(b) a statement indicating a change of medium is inserted in the transferable document or instrument.

(2) Upon issuance of the transferable document or instrument in accordance with this section, the electronic transferable record shall be made inoperative and ceases to have any effect or validity.

(3) A change of medium in accordance with this section shall not affect the rights and obligations of the parties.

34. Non-Discrimination of foreign electronic transferable records.

(1) An electronic transferable record shall not be denied legal effect, validity, or enforceability on the ground that it was issued or used abroad.

(2) Nothing in this Part affects the application to electronic transferable records of rules of private international law governing a transferable document or instrument.

PART VI – CARRIAGE OF GOODS

35. Carriage of goods

(1) This Part applies to any action in connection with or pursuance of a contract of carriage of goods, including:

(a)

(i) furnishing the marks, number, quantity or weight of goods;

(ii) stating or declaring the nature or value of goods;

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b)

(i) notifying a person of terms and conditions of the contract

(ii) giving instructions to a carrier;

(c)

(i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notice of loss or damage to goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating right in goods;

(g) acquiring or transferring rights and obligations under the contract.

(2) Subject to this subsection (1), where the law requires that any action referred to in this Section be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(3) Subsection (2) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(4) If a right is to be granted to, or an obligation is to be acquired by one person and no other person, and if the law requires that in order to effect this, the right or obligation must be conveyed to that person by the transfer or use of a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used.

(5) For the purposes of subsection (4), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(6) Where one or more data messages are used to effect any action in this section, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(7) If a law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by a paper document, that law shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

PART VII – CONSUMER PROTECTION

36. Vendor Information

(1) A service provider or vendor shall provide a consumer with sufficient and relevant information on the products, services, to enable informed decisions on the part of that consumer. Such information shall be:

(a) clearly presented in a language the consumer understands;

(b) accurate;

(c) conspicuously displayed at appropriate stages of the consumer's decision making, particularly before the consumer confirms transactions or provides any personal information; and

(d) capable of being saved or printed by the consumer.

(2) A service provider or vendor shall ensure that its marketing practices and information are current, accurate, not deceptive and misleading to the consumer.

(3) A service provider or vendor shall identify itself and provide information about its business terms, conditions, policies, and practices stating enquiry, complaint and claim procedures, warranty or other support services related to its goods or services before the commencement of the transaction.

(4) Such information mentioned in subsection (3) shall include:

(a) a description of the goods or services including the quantity to be purchased, the full price, including:

(i) the applicable currency;

(ii) any shipping charges, taxes, and specific reference to any other charges that the vendor is responsible for collecting;

(iii) when the vendor cannot reasonably ascertain the amount of potentially applicable charges including additional taxes, customs fees, custom broker fees and the fact that such charges may apply; and

(iv) when the full price cannot be worked out in advance, the method the vendor will use to calculate it, including any recurrent costs and the method used to calculate such costs.

(5) A service provider or vendor shall provide the consumer with a record of the transaction within a reasonable time after the transaction has been completed.

37. Cancellation of contract before processing

(1) A service provider or vendor shall take reasonable steps to ensure that any consumer who agrees to contract is fully informed of terms of such contract. In particular, the consumer shall be provided with an option to correct or cancel the order before it is accepted or processed.

(2) When a service provider or vendor cannot fulfil an obligation to a consumer within the time frame originally specified in the terms of an agreement, the service provider or vendor shall promptly notify the consumer and provide the option of cancelling the order at no charge, except when doing so would be unreasonable.

(3) When a consumer contracts for the ongoing provision of goods or services, and there is a material change in the goods or services, or contract concerning the goods or services, the service provider or vendor shall:

(a) promptly notify the consumer about the change;

(b) provide the consumer with an option to decline further supply of the goods or services, through a simple method of cancellation, without incurring cost or further obligation; and

(c) provide timely confirmation of any such cancellation.

(4) A service provider or vendor shall not hold the consumer liable for any charges related to a transaction in the following circumstances:

(a) the goods or services delivered were materially different from those described by the service provider or vendor;

(b) the service provider or vendor failed to provide material information that could affect the decision about the goods or services;

(c) the goods or services were not delivered in the time specified, or under the conditions stated in the original offer; and

(d) there was no option for the consumer to cancel the transaction when the consumer acted in good faith:

PROVIDED that under these circumstances, a service provider or vendor shall refund any payment(s) the consumer makes, including any reasonable costs the consumer incurred directly in the return of the goods in question to the vendor in good order and within a reasonable time.

38. Consumer's personal information

(1) A service provider or vendor shall ensure confidentiality of all personal information collected from the consumer EXCEPT where the consent of the consumer is obtained or where the law demands disclosure.

(2) A service provider or vendor shall make public its privacy policy and make it easily accessible to the consumer prior to the commencement of the contract and whenever personal information is either requested or collected. Information that shall be disclosed as part of the privacy policy includes the following:

(a) the specific kinds and sources of information being collected and maintained in an electronic form, purposes, usage and disclosure;

(b) the choices available to a consumer regarding the collection, use and disclosure of their personal information, how they may exercise and change these choices, and the implications of such choices;

(c) how a consumer may review and correct or remove such information; and

(d) when the service provider or vendor uses computer cookies, how and why they are used and the consequences of consumers' refusal to accept a computer cookie.

(3) A service provider or vendor shall limit its collection, use and disclosure of personal information to that which a reasonable person would consider appropriate in the circumstances.

(4) A service provider or vendor shall not, as a condition for a transaction, require a consumer to consent to the collection, use or disclosure of personal information beyond that necessary to complete the sale.

(5) When a consumer's consent to the collection, use and disclosure of personal information is required, and cannot reasonably be obtained, such consent shall be provided separately in a clearly worded, online opt-in or opt-out process.

(6) When a service provider or vendor transfers a consumer's personal information to third parties, the service provider or vendor shall remain responsible for the protection of that information. Before any such transfer, the service provider or vendor shall ensure, through contractual or other means that the third party complies with the privacy provisions of the relevant laws in Nigeria.

39. Minimum information in Electronic Commerce

(1) A person using electronic communications to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves including the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number, sufficient to allow–

(a) prompt, easy and effective consumer communication with the seller; and

(b) service of legal process.

(2) A person using electronic communications to sell goods or services to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate record of the information.

(3) A person using electronic communications to sell goods or services to consumers shall provide information about the terms, conditions and costs associated with a transaction in a manner that is accessible, concise, and comprehensive to the consumer, including–

(a) terms, conditions and methods of payment; and details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information;
and

(b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

40. Cyber Insurance

The National Insurance Commission (NAICOM) in consultation with the regulatory agency shall develop and issue regulations including provisions on cyberinsurance to improve security in electronic commerce.

41. Measures on Anti-competitive practices

In order to promote fair competition and practices, the regulatory agency and/or any other entity may inform the Federal Competition and Consumer Protection Commission (FCCPC) of any activities that may violate Anti-competition laws in Nigeria, and the FCCPC shall be obliged to institute a pre-emptive or remedial process where such violation is anticipated or has occurred.

42. Online Dispute Resolution

The regulatory agency in consultation with FCCPC shall develop and issue regulations on online dispute resolution with respect to consumer protection in electronic commerce.

43. Unsolicited messages

Any unsolicited electronic messages sent by a service provider or vendor to a consumer shall prominently display a return address and shall clearly provide a simple procedure by which a consumer can notify the sender that he does not wish to receive such messages.

CHAPTER THREE – DIGITAL TRANSFORMATION IN PUBLIC INSTITUTIONS

PART VIII – DIGITAL GOVERNMENT

44. Use of electronic records and electronic signatures in Government and its agencies

(1) Any public institution that –

(a) accepts the filing of documents, or obtains information in any form;

(b) requires that documents be created or retained;

(c) requires documents, records or information to be provided or retained in their original form;

(d) issues any permit, licence or approval; or

(e) requires payment of any fee, charge or other amount by any method and manner of payment, may carry out such function by electronic form.

(2) Where a public institution conducts its activities or performs its functions by electronic form, the regulatory agency may specify by regulation the following–

(i) the manner and format in which the electronic records shall be filed, created, retained, issued or provided;

(ii) where the electronic records are to be signed, the type of electronic signature required, including, if applicable, a requirement that the sender of the record use a particular type of digital signature;

(iii) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any specified security procedure provider used by the person filing the document;

(iv) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or

(v) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

45. Records available for inspection

Where documents, records or information are required by any law, contract or by deed to be made available for inspection, the requirement shall be met by making such documents, records or information available for inspection as an electronic record.

46. Furnishing of information in prescribed forms.

A legal requirement that a person provide information in a prescribed paper or other non-electronic form to another person is satisfied by providing the information in an electronic form that–

(a) contains the same or substantially the same information as the prescribed paper or other nonelectronic form;

(b) is accessible to the other person to be usable or retrievable for subsequent reference; and

(c) is capable of being retained by the other person.

PART IX – MANAGEMENT AND OPERATIONS OF DIGITAL GOVERNMENT

47. Digital Government structure and processes

The regulatory Agency shall ensure the establishment of digital government governance structure and processes in Federal Public Institutions to govern and control the implementation and proper use of ICT.

48. Establishment of ICT Unit in accordance with the relevant regulations as prescribed by the regulatory agency.

(1) For effective execution of the provisions under this Act, there shall be established in every public institution an ICT Unit with such number of staff as may be required for efficient performance, effective service delivery, and digital transformation of functions in the respective public institution.

49. Digital Government Management

(1) A public institution shall ensure that digital Government initiatives are managed in compliance with guidelines issued by the regulatory agency.

(2) In line with sub-section (1) of this section, a public institution shall, conduct on an annual basis, self-assessment on the implementation of digital-Government initiatives such assessment must be completed on or before the end of the preceding financial year.

(3) A copy of the report mentioned in subsection (2) above shall be submitted to relevant regulatory agency on demand.

(4) Public officers in addition to other requirements for promotion, shall obtain appropriate digital literacy certification relevant to their cadre as may be specified by their employers in consultation with the regulatory agency.

50. Digital Government data management

(1) Public institutions shall comply with electronic data management regulations and publish their information in accordance with open-data principles, as may be prescribed further by the relevant regulatory Agency.

(2) By virtue of this Act, an Information system cadre shall be created in the public service of the federation and in private corporations for the purpose of information security and data management, such Information system cadre shall be accredited under specifications and qualifications provided by the regulatory Agency.

PART X – DIGITAL GOVERNMENT INFRASTRUCTURE AND SYSTEMS

51. Digital Government infrastructure

(1) For the purpose of ensuring that the Government has maximum optimization of infrastructure, public institutions shall use Government approved infrastructure and systems.

(2) For the purpose of ensuring cost effectiveness and ICT readiness, construction of any Government owned infrastructure such as roads, railways, buildings and such other infrastructure shall be subject to the guidelines issued by the relevant authorities-

(a) include ICT Infrastructure as part of the project design in accordance with the appropriate regulation issued by the regulatory agency;

(b) share all the necessary ICT design with the relevant agencies.

52. ICT Projects

(1) Each public institution shall implement ICT projects in compliance with technical standards and guidelines as prescribed by the regulatory agency.

53. Government ICT resources

(1) For the purpose of proper utilization and management of Government-owned ICT resources, public institutions shall:

(a) observe value for money, flexibility in customization, scalability, integration and interoperability in sourcing or using application software;

(b) develop or apply licensed and approved software to conduct their business processes;

(c) ensure Government ICT resources are used for effective public service delivery;

(d) maintain a register of all Government ICT resources owned by the public institution through a central system managed by the regulatory agency; and

(e) acquire government ICT resource specifications guide from the regulatory agency.

PART XI – DIGITAL GOVERNMENT SERVICES

54. Delivery of Digital Government services

A public institution shall, for proper delivery of digital- Government services

(a) use ICT to deliver government services to achieve objectives of the institution;

(b) ensure business processes are reengineered to enhance digital Government service provision;

(c) ensure availability of digital-Government services that are reliable, functional, fitfor- purpose and citizen-centric;

(d) use appropriate channels and languages that enable citizens to access Government services based on available technologies.

(e) make their content and services accessible to all citizens irrespective of the device or platform of their preference.

(f) provide access to functional e-services to persons with disabilities as well as the unserved;

(g) ensure digital - Government services delivered have adequate support systems to end users;

(h) maintain and promote integrated and interoperable systems to be used in service provision; and

(i) Ensure that any business process that facilitates revenue generation is automated and integrated with approved government systems.

(j) avoid duplication of existing databases and source all available data through the data exchange platform of the Federal Government

(k) demonstrate and implement strategies and processes to promote digital literacy for the use of digital services as an essential feature of all digital service offerings or channels.

(l) use Artificial Intelligence (AI) or other emerging technology in compliance with regulations issued by the regulatory authority

55. Reduction of paper documents

Public institutions shall accord preference for digital forms of communication, storing, and processing information by innovating and digitalising processes.

56. Enhancement of electronic records

(1) Where any law provides that records shall be retained for any specific period, that requirement shall be deemed to have been satisfied if such records are retained in electronic form if-

(a) the information contained in that record remains accessible to be usable for a subsequent reference;

(b) the electronic record is retained in the format which represent accurately the information originally generated, sent or received; and

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

(2) The Preservation of public electronic records shall be in accordance with the National Archives Act.

57. Publication of documents in electronic Gazette

(1) Any Public Authority mandated to gazette an information, or a document shall create or make provision for electronic Gazette in accordance with the provisions of this Act.

(2) Where any law provides that any document shall be published in the Gazette, such requirement shall be deemed to have been satisfied if such document is published in an electronic Gazette.

58. Electronic communication of Government

(1) Where any law provides for

(a) the sending of any letter, request, report, internal memo or any other document within Government office, authority, body or agency in a particular manner; and

(b) the issuing of messaging, or any other form of multimedia communication within the Government offices or officials, such communication shall be deemed to have been met if effected by means of electronic form.

(2) All Public institutions shall provide effective communication and contact channels to support service delivery to the public.

(3) The relevant authority shall for the purpose of sub-section 1 and 2, prescribe:

(a) the standards of the approved systems and devices to be used for official Government Communication;

(b) the category, type, classification of information and data that shall be transmitted through electronic communication, without prejudice to any law that provides for official classification of government information;

(c) the category, type, classification of information and data that shall not be transmitted through electronic communication.

59. Audit of documents in electronic form

Where any law provides for audit of documents, records or information, that law shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

60. Delivery of services by service provider

For the purposes of efficient service delivery, Bureau of Public Procurement (BPP) and the regulatory agency in collaboration with other relevant agencies shall issue regulatory frameworks for delivery of quality digital services.

CHAPTER FOUR – GENERAL PROVISIONS

PART XII – OFFENCES AND CONTRAVENTIONS

61. Offences and penalties

(1) Except as otherwise provided in this Act, any person or corporate body who contravenes or fails to comply with the provisions of this Act commits an offence.

(2) Where an offence under this Act is committed by a body corporate or firm or other association of individuals:

(a) Every Chief Executive Officer of the body corporate or any officer acting in that capacity or on his behalf; and

(b) Every person purporting to act in any capacity mentioned under paragraph (a) of this subsection (2) commits an offence, unless the person proves that the act or omission constituting the offence took place without his knowledge, consent or connivance.

(c) A body corporate, firm or other association of individuals who commits an offence under this Act is liable on conviction, to a fine not less than N10,000,000.00.

(3) Where a person or body corporate fails to comply with the frameworks, guidelines, regulations, standards, circulars, directives or administrative sanctions prescribed by the Agency in the discharge of its duties under this Act, such person commits an offence and is liable on conviction to a fine of not less than N 1,000,000.00 and not less than N10,000,000 for a body corporate.

(4) The regulatory authority shall collaborate with all the relevant ministries, departments, agencies or establishments to enforce guidelines, standards and any other provisions formulated in the discharge of its duties under the Act.

Except as otherwise provided in this Act, a body corporate or person who commits an offence under this Act where no specific penalty is provided, is liable on conviction:

(a) For a first offence, a fine not less than N1,000,000 for a person and N10,000,000 for a body corporateor both such fine ; and

(b) For a second and subsequent offence, a fine of not less than N3,000,000 for a person or N30,000,000 for a body corporate.

(5) The institution of proceedings or imposition of a penalty under this Act shall not relieve a body corporate from liability to pay to the Federal Inland Revenue Service such levy or tax which may become due under this Act.

PART XIII – MISCELLANEOUS

62. Supremacy of National Digital Economy and E-Governance Act

(1) Notwithstanding the provisions of any other law but subject to the provisions of the Constitution of the Federal Republic of Nigeria, in all matters relating to digital economy and e-government, the provisions of this Act shall override the provisions of any other Law.

(2) In so far as this Act applies to an industry or sector of an industry that is subject to the jurisdiction of another government agency by the provisions of any other law, in matters or conducts which affect the digital economy and electronic government, this Act shall be construed as establishing a concurrent jurisdiction between the regulatory agency and the relevant public institution, with the regulatory agency having precedence over and above the relevant public institution.

(3) The regulatory agency shall negotiate agreements with any public institution whose mandate includes enforcement of digital economy and e-government for the purpose of coordinating and harmonising the exercise of jurisdiction over digital economy and electronic government matters within the relevant industry or sector, and to ensure the consistent application of the provisions of this Act.

(4) Where the negotiations contemplated by subsections (3) are inconclusive, the areas of disagreement shall be referred to the Attorney General and Minister of Justice in the case of a large merger, for advice on public interest grounds.

63. Other Regulations

(1) The regulatory agency in consultation with the relevant Stakeholders shall determine, insert, and publish digital literacy skill sets for Nigerians at various levels to be implemented through national curriculum at all levels in both the public and private sectors.

(2) Government procurement processes as may be determined by Bureau of Public Procurement shall accommodate the use of sandboxes for the testing and adoption of new and emerging technologies in public service.

(3) The regulatory agency shall establish regulations on the use and adoption of new and emerging technologies as it relates to information technology.

PART XVI - INTERPRETATION

In this Act, unless the context otherwise requires–

“addressee”, in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication;

“authentication data” includes username, password and license key;

“automated system” means a computer programme or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by an individual each time an action is initiated, or a response is generated by the program or electronic or other means;

“certificate” means a data message or other record confirming the link between a signatory and the signature creation data;

“consumer” means any person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier;

"critical application software" means application software which is used to deliver or perform core institutions or Government business processes;

"critical system" means a system which is used to deliver or perform core institutions or Government business processes;

"data" means any information presented in an electronic form;

“data message” means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy;

“digital signature” means a signature that fulfils the requirements of Section 21;

“electronic” or “e” includes electrical, digital, magnetic, wireless, optical, electro-magnetic, biometric, photonic and similar capabilities;

“electronic-commerce service provider” means a person who uses electronic means in providing goods or services or both;

"electronic communication" means any transfer of sign, signal, information or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, photo optical or in any other similar form that is processed, recorded, displayed, created, stored, generated, received or transmitted in an electronic form;

“electronic form” with reference to information, means any information generated, sent, received or stored in media, magnetic form, optical form, computer memory, microfilm, computer generated microfiche or similar device;

“electronic Government” or "e-Government" means the use of information and communication technologies (ICT) by the Government to deliver public services;

"e-Government initiative" means any intervention taken by public institution for the purpose of implementing e- government;

"e-Government security" means ICT security in the public sector;

"e-Government services" means all services which are delivered by public institutions by electronic means;

“electronic record” means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another;

“electronic signature” means data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign;

"electronic transaction" includes transmission of data, information, document or providing services electronically.

“electronic transferable record” means an electronic record that complies with the requirements of section 31;

“entity” means a partnership or body, whether corporate or unincorporated, engaged in business;

"government ICT resources" includes ICT equipment,software, bandwidth, documents and other ICT related resources;

"ICT infrastructure" includes composite hardware, software, network resources and services required for the existence, operation and management of an enterprise ICT environment;

"ICT project" includes a project for acquiring, sourcing or improving ICT infrastructure or systems for undertaking e-Government initiatives;

"ICT system" includes an ICT set-up consisting of hardware, software, data, communication technology and people who use them;

"ICT security" includes protecting information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability;

"ICT unit" includes directorate, department or unit responsible for ICT matters in the public institution;

“individual” means a natural person;

“information” includes data, text, documents, images, sounds, codes, computer programmes, software and databases;

“information system” includes a system for generating, sending, receiving, storing or otherwise processing an electronic record;

“intermediary”, with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives, transmits or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication, and includes telecommunication service providers, network service providers, internet service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafés;

"interoperability" means the ability of different information technology systems and software applications to communicate, exchange data and use of information that has been exchanged;

"metadata" means a set of data that describes and provides information about other data;

“originator” in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication;

"public institution" Means ministries, departments, agencies, executive agencies, parastatals, organizations, public corporations or any other Government autonomous or semi-autonomous institutions;

“record” includes information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;

“regulatory agency” Means the National Information Technology Development Agency.

“relevant agency” Means any agency authorised by its mandate to carry out a particular function.

“security procedure” means a procedure established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that an electronic signature, communication or performance is that of a particular person or for detecting changes or errors in content of an electronic communication;

"service provider" means an organization, business or individual which offers electronic service to a public institution;

“signatory” means an individual who creates an electronic signature;

“signed” or “signature” and its grammatical variations mean a method (electronic or otherwise) used to identify a person and to indicate the intention of that person in respect of the information contained in a record;

“signature creation data” means unique data, including codes or private cryptographic keys or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

“specified security procedure” means a security procedure which is specified by the regulatory Agency NITDA;

“specified security procedure provider” means a person involved in the provision of a specified security procedure;

“time stamp” means a data unit created using a system of technical and organisational means which certifies the existence of electronic data at a given time;

“transaction” means an action or set of actions relating to the conduct of business, consumer or commercial affairs between two or more persons including the sale, lease, exchange, licensing or other disposition of personal property, including goods and intangible interests in real property, services or any combination of any of these acts;

“transferable document or instrument” mean a document or instrument issued on paper that entitles the holder to–

(a) claim the performance of the obligation indicated in the document or instrument; and

(b) transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.

1. "place of business", in relation to a party, means–

(a) any place where the party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location; or

(b) if the party is an individual and he does not have a place of business, the person's habitual residence.

2. For the purposes of sub-section (1)

(a) if a party has indicated his place of business, the location indicated by him is presumed to be his place of business unless another party proves that the party making the indication does not have a place of business at that location;

(b) if a party has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract;

(c) a location is not a place of business merely because that location is–

(i) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(ii) where the information system may be accessed by other parties; and

(d) the sole fact that a party makes use of a domain name, or an electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

3. Where an electronic communication does not relate to any contract, references to a contract in sub-section (2) shall refer to the relevant transaction.

Short Title
National Digital Economy and E-Governance Act