ELECTRONIC TRANSACTIONS BILL, 2025

ARRANGEMENT OF SECTIONS

Section

Object and scope of the Act

A BILL

ENTITLED

ELECTRONIC TRANSACTIONS ACT, 2025

AN ACT to provide for the regulation of electronic communications and related transactions and to provide for related matters.

DATE OF ASSENT:

ENACTED by Parliament and assented to by the President

Object of the Act

Object of the Act

1. (1) The object of this Act is to provide for and facilitate electronic communications and related transactions in the public interest, and to

(a) remove and prevent barriers to electronic communications and transactions;

(b) promote legal certainty and confidence in electronic communications and transactions;

(c) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

(d) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(e) promote the development of electronic transaction services responsive to the needs of consumers;

(f) ensure that, in relation to the provision of electronic transactions services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account;

(g) ensure compliance with accepted international technical standards in the provision and development of electronic communications and transactions; and

(h) ensure that the interest and image of the Republic are not compromised through the use of electronic communications.

Application

2. This Act applies to electronic transactions and electronic records of every type.

Scope of Act

3. (1) This Act shall not be interpreted so as to exclude statutory law or the principles of the common law being applied to, recognising or accommodating electronic transactions, electronic records or any other matter provided for in this Act.

(2) Unless otherwise provided, this Act shall not be construed as

(a) requiring a person to generate, communicate, produce, process, send, receive, record, retain, store or display information, document or signature by or in electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept electronic records.

(3) This Act does not limit the operation of law that expressly authorises, prohibits or regulates the use of electronic records and any legal requirement law for information to be posted, displayed or transmitted in a specified manner.

Electronic transactions

Recognition of electronic message

4. Except as provided in this Act, where a law provides that information or any other matter shall be in writing, typewritten or in printed form, the requirement shall be deemed to have been satisfied if the information or matter is

(a) rendered or made available in an electronic form,

(b) accessible, and

(c) capable of being retained for a subsequent reference despite the contrary intention in the law.

Original writing

5. (1) Where a law requires information to be presented or retained in its original form, the requirement shall be deemed to have been satisfied by an electronic record if

(a) there is reliable assurance of the integrity of the electronic record, and

(b) the electronic record is capable of being displayed to the person to whom it is to be presented.

(2) The criteria to assess integrity shall be whether the information has remained complete and unaltered and the information shall be assessed taking into consideration the relevant circumstances for which the information was generated to determine the standard of reliability.

Admissibility and evidential weight of electronic records

6. (1) The admissibility of an electronic record shall not be denied as evidence in legal proceedings except as provided in this Act.

(2) In assessing the evidential weight of an electronic record the Court shall have regard to

(a) the reliability of the manner in which the electronic record was generated, displayed, stored or communicated,

(b) the reliability of the manner in which the integrity of the information was maintained,

(c) the manner in which its originator was identified, and

(d) any other facts that the Court may consider relevant.

Retention of electronic records

7. (1) Where a law requires that a document, record or information shall be retained, that requirement is deemed to have been met if the document, record or information is held in electronic form and

(a) is accessible,

(b) is capable of retention for subsequent reference,

(c) 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

(d) is retained to enable the identification of the origin and destination of the electronic record and the date and time when it was sent or received.

(2) The document, record or information shall be kept in electronic form for at least six years.

(3) An obligation to retain a document, record or information does not extend to information which is only to enable the message to be sent or received.

Secure electronic record

8. (1) Where a security procedure has been applied to an electronic record at a specific point in time, the record is deemed to be a secure electronic record during the period when the security procedure was applied.

(2) An unauthorised alteration of the security procedure renders the record invalid.

(3) An alteration is unauthorised if it is done by a person without the lawful authority of the person who originally applied the security procedure.

Digital and electronic signatures

9. (1) Where a law requires the signature of a person, that requirement is deemed to be satisfied in relation to an electronic record if a digital or electronic signature is used.

(2) A digital or electronic signature is deemed to be authentic if

(a) the means of creating the digital or electronic signature is, within the context in which it is used, linked to the signatory and not to another person,

(b) the means of creating the digital or electronic signature was, at the time of signing, under the control of the signatory and not another person without duress or undue influence,

(c) an alteration to the digital or electronic signature, made after the time of signing, is detectable

(3) Subsection (2) does not limit the right of a person

(a) to prove the authenticity of a digital or electronic signature in any other way, or

(b) to adduce evidence in respect of the non-authenticity of a digital or electronic signature.

(4) Digital and electronic signature certificates shall be issued only upon the conduct of rigorous identity verification, including but not limited to biometric authentication and validation against a national identification database, in accordance with the provisions of the National Identification Authority Act, 2006 (Act 707), any Regulations made thereunder, or any other applicable enactments for the time being in force.

Equal treatment of digital and electronic signatures

10. Except as provided in this Act, the provisions of this Act do not exclude, restrict, or deprive of legal effect, any method of creating a digital or electronic signature which

(a) satisfies the requirements of this Act,

(b) meets the requirements of other statutory provision, or

(c) is provided for under a contract.

Signing of an electronic record

11. A person may sign an electronic record by affixing a personal digital or electronic signature or using any other recognised, secure and verifiable mode of signing agreed by the parties or recognised by the industry to be safe, reliable and acceptable.

Conduct of a person relying on a digital or electronic signature

12**.** A person who relies on a digital or electronic signature shall bear the legal consequences of failure to

(a) take reasonable steps to verify the authenticity of a digital or electronic signature, or

(b) take reasonable steps where a digital or electronic signature is supported by a certificate, to

(i) verify the validity of the certificate, or

(ii) observe any limitation with respect to the certificate.

Recognition of digital certificates and digital and electronic signatures

13**.** (1) Unless otherwise prescribed by law, a person may determine the digital or electronic signature, certificate or authentication the person will use.

(2) The Minister may recognise a digital or electronic signature, certificate or authentication of a foreign information security service provider for use by a public servant by notice published in the *Gazette.*

Notarisation, acknowledgement and certification

14**.** (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is deemed to be satisfied if the electronic or digital signature of the person authorised to perform those acts is affixed to an electronic record.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or in another physical form, that requirement is deemed to be satisfied if an electronic copy of the document is certified to be a true copy by using the electronic or digital signature of the certifying person.

Other requirements

15**.** (1) A requirement in law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single electronic record that is capable of being reproduced by the addressee.

(2) Where a corporate seal is required to be affixed to a document, that requirement is deemed to be satisfied if the electronic or digital signature of the corporate body is affixed to the electronic record in accordance with the provisions relating to the use of the corporate seal.

Automated transactions or decision-making

16**.** (1) A platform or service provider that uses automated decision-making, including algorithmic curation, profiling, or recommendation systems, shall

(a) ensure transparency of the system by disclosing key parameters, logic and potential impacts;

(b) provide users with meaningful information on how such systems affect access to goods, services, or content;

(c) allow users to opt-out of personalised recommendations, where feasible.

(2) The Minister may issue guidelines or regulations for the ethical use of artificial intelligence and automated systems, having regard to fairness, accountability, transparency, and non-discrimination.

(3)An automated transaction is valid even if an electronic agent is involved at any stage of its formation.

(4) A party interacting with an electronic agent to make an agreement is not bound by the terms of the agreement unless the terms were capable at first of being accessed by the party prior to the formation of the contract.

(5) An electronic contract is not valid where an individual interacts directly with the electronic agent and has made a material error during the creation of an electronic record and

(a) the electronic agent did not provide that person with an easy opportunity to prevent or correct the error;

(b) that person notifies the party creating the electronic record of the error as soon as practicable after noticing it;

(c) that person takes reasonable steps to return to the previous situation; and

(d) that person has not used or received material benefit or value from performance received from the other person.

Despatch of electronic record

17**.** Unless otherwise agreed between the originator and the addressee, the despatch of an electronic record occurs when it enters an information processing system outside the control of the originator or the agent of the originator.

Receipt of electronic record

18**.** The time of receipt of an electronic record shall be determined as follows

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs at the time when the electronic record enters the designated information system; or

(b) if the addressee has not designated an information system, receipt occurs when the electronic record enters an information

system of the addressee through which the addressee retrieves the electronic record.

(2) An electronic record is deemed to be despatched at the originator's registered place of business and is deemed to be received at the registered place where the addressee has its place of business unless otherwise agreed by the originator and the addressee.

Expression of intent or other statement

19**.** An expression of intent or other electronic representation of an electronic record between the originator and the addressee of an electronic record is admissible in circumstances where the intent or other electronic representation is relevant in law.

Attribution of electronic records to originator

20**.** (1) An electronic record is considered to be that of the originator if it was sent by

(a) the originator personally;

(b) a person who has authority to act on behalf of the originator in respect of that electronic record; 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 the programme.

(2) An addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption, if

(a) the addressee properly applied a procedure previously agreed with the originator in order to ascertain whether the electronic record was that of the originator; or

(b) the electronic record received by the addressee resulted from the actions of a person whose relationship with the originator or with an agent of the originator enabled that person to gain access to a method used by the originator to identify an electronic record as the originator's own.

(3) Where a procedure has not been agreed by both parties to ascertain the originator, the person who appears to be the originator shall be presumed to be the originator.

(4) The presumption in subsection (3) does not apply where

(a) the addressee has received notice from the originator that the electronic record was issued without the knowledge or consent of the originator;

(b) the addressee knew or should reasonably have known, or used any agreed procedure to know that the electronic record was not that of the originator and that the person who sent the electronic record did not have the authority of the originator to issue or send the electronic record; or

(c) the addressee knew or should reasonably have known, that the transmission resulted in an error in the electronic record as received.

Acknowledgement of receipt of electronic record

21**.** (1) An acknowledgement of receipt may be given through

(a) a communication by the addressee, whether automated or otherwise; or

(b) any conduct of the addressee to indicate to the originator that the electronic record has been received.

(2) An acknowledgement of receipt is not necessary to give legal effect to a message unless otherwise agreed by the parties.

Formation and validity of agreements

22**.** An agreement is valid even if it was concluded partly or in whole through an electronic medium.

Variation by agreement between parties

23**.** Sections 4 to 22 only apply if the parties involved in generating, sending, receiving, storing or otherwise processing electronic records have not agreed on the issues provided for by these sections.

Electronic government services

Acceptance of electronic filing and issuing of documents

24. A public body shall take steps or enter into arrangements to ensure that its functions are carried out, delivered or accessed electronically or online.

Public agency and electronic records

25. (1) A public agency that, pursuant to any law accepts the filing of documents, requires that documents be created or retained, issues a permit, licence or approval or provides for a payment in accordance with law, shall

(a) accept the filing of a document, or the creation or retention of documents in the form of an electronic record;

(b) issue the permit, licence or approval in the form of an electronic record; or

(c) make or receive payment in electronic form or by electronic means.

(2) Any public agency may specify by notice in the *Gazette:*

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

(b) the type of electronic or digital signature required where the electronic record has to be signed;

(c) the manner and format in which an electronic or digital signature shall be attached to, incorporated in or otherwise associated with the electronic record;

(d) the identity or criteria required of an authentication service provider used by the person filing the electronic record or the public agency may designate an authentication service provider as a preferred authentication service provider;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(f) any other requirements for electronic records or payments.

Publication in electronic format

26. (1) Where a law requires publication in the *Gazette* the requirement is deemed to have been satisfied if published in electronic format referred to as an *E-Gazette.*

(2) The date of publication is deemed to be the date of first publication in the *Gazette.*

(3) Despite any other enactment, the E-Gazette shall have the same legal force and effect as the printed version of the Gazette.

(4) The E-Gazette shall be admissible in all judicial, quasi-judicial and administrative proceedings as conclusive evidence of the contents therein, without further proof of authenticity, where it bears a valid electronic or digital signature issued under this Act.

Certifying Agency

Prohibited acts

27. A person shall not sell or provide encryption or authentication service contrary to the provisions of this Act.

Provision of authentication encryption services

28. An encryption or an authentication service or product is deemed to have been provided in the country if it is made available

(a) from premises within the country;

(b) from a body incorporated in the country;

(c) to a person who is present or operating from any system in the country when that person makes use of the service or product; or

(d) from a Ghanaian associated or related domain name or website.

Certifying Agency

29. (1) The National Information Technology Agency established under National Information Technology Agency Act … (Act …) shall serve as the Certifying Agency under this Act.

(2) The Certifying Agency shall maintain a website and provide information at the website in accordance with this Act.

Functions of the Certifying Agency

30. (1)The functions of the Agency are to:

(a) issue licences for encryption and authentication service;

(b) monitor the conduct, system and operation of encryption and authentication service providers to ensure compliance with conditions of the licence, and the provisions of this Act;

(c) suspend a licence of a licence holder;

(d) revoke a licence of a licence holder; and

(e) appoint, accredit and gazette independent auditing firms to conduct periodic audits of a licence holder to ensure

compliance with the terms and conditions of any licences issued under this Act.

(2) The Agency shall publish and maintain on its official website a list of accredited auditors, duly certified in accordance with the provisions of this Act and any Regulations made thereunder.

Revocation or suspension of licence

31. (1) The Agency may suspend or revoke a licence if it is satisfied that the authentication service provider has failed or ceased to meet any of the requirements, conditions or restrictions subject to which the licence was granted or recognition was given.

(2) The Agency shall not suspend or revoke a licence unless it has

(a) notified the licence holder in writing of its intention to do so,

(b) given a description of the alleged breach, and

(c) afforded the licensed holder the opportunity to

(i) respond to the allegations in writing, and

(ii) remedy the alleged breach.

(3) The Agency may suspend a licence with immediate effect for a period not exceeding ninety days pending implementation of the procedures required to remedy the breach where there is the likelihood of irreparable harm to consumers or third parties involved in an electronic transaction.

(4) A licence holder may surrender the licence to the Agency subject to the provisions of the licence and third party rights.

(5) The Agency shall publish the suspension or revocation of a licence on its website.

Surrender of licence

32. (1) A licensee with a suspended or revoked licence shall surrender the licence to the Agency within twenty-four hours of receipt of notice of the suspension or revocation of its licence.

(2) Where a licensee fails to surrender the licence, each director of the licensee commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units for each day that the licence is not surrendered or to a term of imprisonment of not more than two years or to both.

Recognition of foreign certifying authorities

33. (1) Subject to the conditions and restrictions that may be specified by law, the Agency may, by notification in the *Gazette,* recognise a foreign entity as a certifying agency.

(2) An electronic or digital signature or certificate issued by a foreign certification service provider shall have the same legal effect as a signature or certificate issued under this Act, if

(a) the foreign certification service provider operates under a regime that provides substantially similar levels of trust and reliability; or

(b) the certificate is recognised by the Certifying Agency through mutual recognition arrangements or approved interoperability frameworks.

(3) The Minister may, by legislative instrument, specify the countries, regimes or classes of certificates deemed to offer substantially equivalent assurance.

(4) Where a foreign entity is recognised, as a certifying agency, service and products issued by a person pursuant to the directives of that foreign certifying agency are valid.

(5) The Agency by notification in the *Gazette* may revoke the recognition if it is satisfied that a foreign certifying agency has contravened any of the conditions and restrictions subject to which it was granted recognition.

(6) The National Information Technology Authority, as the designated certifying agency, shall develop and publish a regulatory framework for the mutual recognition of foreign certifying authorities.

(7) A foreign certifying authority that seeks recognition under the framework referred to in subclause (4) shall comply with

(a) the interoperability standards prescribed under the framework; and

(b) applicable international best practices on electronic certification

Repository of digital and electronic signatures

34. (1) The Agency shall be the repository of Digital and Electronic Signature Certificates issued under this Act.

(2) The Agency shall

(a) make use of hardware, software and procedures that are secure from intrusion and misuse; and

(b) observe other standards that may be prescribed, to ensure that the secrecy and security of digital or electronic signatures are assured.

(3) The Agency shall maintain a computerised data base of the public keys to make them verifiable by a member of the public.

Register of licence holders

35. (1) The Agency shall establish and maintain a register of licence holders.

(2) The Agency shall record the following particulars in respect of each licence holder

(a) the name and address of the licence holder;

(b) a description of the type of service or product provided;

(c) other particulars that may be prescribed to identify and locate the license holder or its products or services;

(d) licensed encryption and authentication products or services under this Act;

(e) licensed encryption and authentication products and services recognised under this Act;

(f) suspended and revoked licences or recognition; and

(g) any other information that may be prescribed or may be deemed appropriate by the Agency.

(3) The Agency shall provide notice of the suspension or revocation at its website.

(4) The Agency shall publish the list of licence holders, revoked or suspended licences in electronic and other media, subject to the rules relating to confidentiality.

(5) A licence holder shall not be required to disclose confidential information or trade secrets in respect of its products or services.

Restrictions on disclosure of information

36. Subject to the provisions of the Constitution, a person may disclose information under this Act

(a) to a law enforcement agency;

(b) for criminal or civil proceedings;

(c) to government agencies responsible for safety and security on official request; and

(d) to a third party enquiry for confirmation of a licence or representations made by a licence holder.

Application for licence

37. (1) A licence shall not be issued or granted by the Agency to an individual.

(2) Each application for the issue of a licence shall be in the prescribed form.

(3) A licence issued under this Act shall not be assigned, transferred, sub-licensed, or otherwise disposed of, whether wholly or partly, to any other person or entity, except with the prior written approval of the Agency and subject to any terms and conditions that may be prescribed.

(4) Each application for a licence shall be accompanied with,

(a) a certificate of incorporation,

(b) a statement including the procedures with respect to the identification of the applicant.

(c) payment of a non-refundable application fee, and

(d) other prescribed documents.

(5) The Agency shall, in considering an application for a licence, take into account the following

(a) the financial and human resources available to the applicant, including its capital and other assets;

(b) the quality, reliability, and security of the applicant's hardware and software systems;

(c) the adequacy and integrity of the applicant's procedures for processing its products or services;

(d) the availability of accurate and timely information to third parties relying on the authentication product or service;

(e) the regularity and extent of audits conducted by an independent body;

(f) the technical and other requirements to be met by certificates issued by the licence holder;

(g) the procedures and standards applicable to the issuance of certificates;

(h) the requirements relating to certification practice statements;

(i) the responsibilities of the certification service provider;

(j) the liability of the certification service provider;

(k) the nature and format of records to be maintained, and the manner and duration for which such records shall be kept;

(l) the procedures governing certificate suspension and revocation;

(m) the procedures for notification of certificate suspension and revocation;

(n) any other conditions, restrictions, or factors as may be prescribed or as the Agency may consider necessary or appropriate; and

(o) the applicant's compliance with any minimum capital requirement prescribed by the Agency.

(6) A licence is valid for the period and on the terms and conditions that may be determined by the Agency.

Grant of licence

38. (1) The Agency shall not grant a licence under this Act unless the Agency is satisfied that a security procedure related to or issued by an applicant,

(a) is uniquely linked to the user;

(b) is capable of identifying that user;

(c) is created using means that can be maintained under the sole control of that user; and

(d) will be linked to the electronic record to which it relates so that any subsequent change of the electronic record is detectable.

(2) The Agency may, prior to licensing any authentication products or services, stipulate

(a) the technical and other requirements to be met by certificates issued by the licence holder;

(b) the requirements for issuing certificates;

(c) the requirements for certification practice statements;

(d) the responsibilities of the certification service provider;

(e) the liability of the certification service provider;

(f) the records to be kept and the manner in which and length of time for which they must be kept;

(g) requirements concerning certificate suspension and revocation procedures;

(h) requirements as to notification procedures relating to certificate suspension and revocation; and

(i) other conditions or restrictions that the Agency may consider necessary.

(3) A licence is not transferable.

Display of licence

39. A licensee shall display its licence conspicuously on the premises of its principal place of business.

Duties of licensed entities

40. A licensee shall

(a) ensure that each person employed or engaged by it complies with the provisions of this Act, Regulations made under this Act and the licence conditions;

(b) obtain and maintain liability insurance coverage, with a minimum coverage amount of Ten Million Ghana Cedis (GHS 10,000,000.00), or such other amount as may be prescribed by the Agency;

(c) compensate subscribers for any loss or damage arising from

(i) the issuance of fraudulent certificates; or

(ii) the failure to promptly revoke compromised certificates; or

(iii) from any act or omission of the licensee in breach of its obligations under this Act or any Regulations made under the Act.

Renewal of licence

41. An application for renewal of a licence shall be

(a) in the form prescribed by the Agency, and

(b) accompanied with the fees prescribed and shall be paid in full before the issue of a licence.

Procedure for grant or rejection of renewal of licence

42. (1) The Agency may grant or reject the application for the renewal after considering the documents accompanying the application for renewal and other factors considered necessary.

(2) The Agency shall provide reasons for the rejection of the application in writing to the applicant.

Notification of adverse event

43. (1)The Agency shall

(a) use reasonable efforts to notify any person who is likely to be affected by the occurrence of an adverse event; or

(b) deal with the event or situation in accordance with the procedure specified in its certification practice statement

where in the opinion of the Agency an event has occurred or a situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a licence was granted.

(2) A licensee or certifying authority shall, within twenty-four hours of the occurrence or discovery of a breach or suspected breach affecting the security or integrity of its systems or services, submit its Incident Response Plan to the Agency in the form and manner prescribed by the Agency.

Procedures to be followed by licensed person

44. A licensed person shall

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide such level of reliability in its services which are reasonably suited to the performance of the intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the product or service are assured; and

(d) adhere to such security procedures and observe such other standards as may be prescribed.

Consumer protection

Scope of application

45. Sections 46 to 53 apply only to electronic transactions.

Information to be provided

46. (1) A supplier offering goods or services for sale, hire or exchange in an electronic transaction shall make available to the consumer on the electronic platform where the goods or services are offered the following information related to the supplier

(a) full name and legal status;

(b) physical address and telephone number;

(c) website address and e-mail address;

(d) membership of any self-regulatory or related bodies and the contact details of the body;

(e) a code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;

(f) the registration number, the names of office bearers and the place of registration of the supplier as a legal person;

(g) sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;

(h) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(i) the manner of payment;

(j) terms of agreement including guarantees that will apply to the transaction and how these terms may be accessed, stored and reproduced electronically by consumers;

(k) the time within which the goods will be despatched or delivered or within which the services will be rendered;

(l) the manner and period within which consumers can access and maintain a full record of the transaction;

(m) the return, exchange and refund policy;

(n) the alternative dispute resolution code to which that supplier subscribes and access to the code by the consumer;

(o) the security procedures and privacy policy of that supplier as regards payment, payment information and personal information;

(p) the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently where appropriate; and *(q)* the rights of consumers as provided for in this section.

(2) The supplier shall provide a consumer with an opportunity to

(a) read, store and reproduce the contract terms and general conditions;

(b) identify and correct handling errors; and

(c) withdraw from the transaction before concluding a contract.

(3) If a supplier fails to comply with the provisions of this section, the consumer may cancel the contract within fourteen days of receipt of the goods or services under the transaction.

(4) If a transaction is cancelled as a result of the failure of the supplier to comply with the provisions of this section

(a) the consumer shall return the goods received, or where applicable, cease using the services performed; and

(b) the supplier shall refund payments made by the consumer within thirty days.

(5) The supplier shall utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) The supplier is liable for damage suffered by a consumer due to failure by the supplier to apply a secure payment system.

Performance

47. (1) The supplier shall execute the order within fourteen days after the day on which the supplier receives the order, unless the parties have agreed otherwise.

(2) Where a supplier fails to execute the order within the fourteen days or within the agreed period, the contract is voidable.

(3) If a supplier is unable to perform on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payment within seven days after the date of notification.

Grace period

48. (1) A consumer is entitled to cancel a transaction and any related credit agreement for the supply

(a) of goods within fourteen days after the date of the receipt of the goods; or

(b) of services within seven days after the date of the conclusion of the agreement,

without reason and without penalty.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) This section shall not be construed to limit the rights of a consumer provided for in any other law.

(4) This section does not apply to an electronic transaction

(a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;

(b) by way of an auction;

(c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;

(d) for services which began with the consumer's consent before the end of the seven-day grace period;

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) where the goods

(*i*) are made to the consumer's specification,

(*ii*) by reason of their nature cannot be returned, or

(*iii*) are perishable;

(g) where audio or video recordings or computer software were unsealed by the consumer;

(h) for the sale of newspapers, periodicals, magazines and books;

(i) for the provision of gaming and lottery services; or

(j) for the provision of accommodation, transport, catering or leisure services where the supplier has commenced the provision of these services on a specific date or within a specific period.

Unsolicited goods, services or communications

49. (1) Except in the case of a notice sent by an electronic communications provider to a customer in relation to the service, a person shall not send unsolicited electronic communications to a consumer without obtaining the prior consent of the consumer.

(2) A person who sends electronic commercial communication to a consumer shall provide the consumer

(a) with the option to cancel the subscription to the mailing list of that person, and

(b) with the identifying particulars of the source from which that person obtained the consumer's personal information at the request of the consumer.

(3) An agreement shall not be deemed to have been concluded where a consumer fails to respond to an unsolicited communication; and the consumer is entitled to recover the costs associated with the cancellation of unsolicited communication.

(4) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

(5) A person who sends unsolicited commercial communications to another person or who continues to send unsolicited commercial communications after cancellation of the subscription commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

Liability for misuse of electronic payment medium

50. (1) A holder of an electronic payment medium shall not, unless acting in collusion with another person, be liable to the issuer for loss arising from use of the medium by a person who is not acting or being treated as acting as the agent of the holder.

(2) Subsection (1) does not prevent

(a) the holder of the electronic payment medium from being made liable for loss to the issuer arising from use of the medium by another person during a period beginning when the medium ceases to be in the possession of an authorised person and ending when the medium is once more in the possession of an authorised person; or

(b) the holder from being made liable to any extent for loss to the issuer from use of the medium by a person who acquired possession of it with the holder's consent.

(3) Subsections (2) does not apply to the use of the electronic payment medium after the issuer has been given notice of loss and does not

apply unless the issuer provides the holder with particulars of the name, address and telephone number of a person stated to be the person to whom notice is to be given.

(4) The notice takes effect when received, but where it is given orally, shall be confirmed in writing within fourteen clear days.

(5) A sum paid by the holder for the issue of the electronic payment medium is treated as paid towards satisfaction of liability under this section to the extent that it has not been previously offset by use made of the medium.

(6) The holder or a person authorised by the holder to use the electronic payment medium is an authorised person for the purpose of subsection (2).

Electronic payment medium lists prohibited

51. (1) A financial institution shall not

(a) make available;

(b) lend; or

(c) sell any list or portion of a list of holders of an electronic payment medium and their addresses and account numbers to any person without the prior written consent of the holders except by order of a Court.

(2) A financial institution may make available to another financial institution information about an electronic payment medium holder's credit rating without the holder's prior written consent if written notice of the disclosure is given to the holder within seven days subject to any law regulating credit rating institutions.

(3) A financial institution which contravenes subsection (1) commits an offence and each director and officer of the institution who fails to ensure compliance with this Act is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or imprisonment for a term of not more than five years or to both.

Applicability of foreign law

52. Despite a provision of an agreement to the contrary, the supply of goods pursuant to a contract to consumers in this country is subject to the provisions of this Act.

Non-exclusion

53. A provision in an agreement which excludes consumer rights provided for in this Act is void.

Protected computers and critical database

Protected computer

54. (1) The Minister may declare that a computer, computer system or computer network is a protected system by notification in the *Gazette*.

(2) The Minister may authorise access to a protected system by or in writing.

(3) Until the Minister by *Gazette* publication declares a computer, computer system or computer network to be a protected system, the computer ,computer system or computer network shall be treated as a "protected computer" if the computer, program or electronic record is used directly in connection with or for

(a) the security, defence or international relations of the country;

(b) the existence or identity of a confidential source of information related to the enforcement of criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure;

(d) the protection of public safety and public health, including systems related to essential emergency services;

(e) foreign commerce or communication affecting a citizen of Ghana or business in which a citizen of Ghana or the Government has an interest; or

(f) the legislative, executive or judicial service, the public services and security agencies.

(4) A person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or imprisonment for a term of not more than ten years or to both.

Identification of critical electronic record and critical databases

55. The Minister may by notice in the *Gazette*

(a) declare certain classes of information which are of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical electronic records for the purpose of this Act; and

(b) establish a procedure to be followed in the identification of critical databases for the purposes of this Act.

Scope of critical database protection

56. The Minister may declare certain classes of information relating to national security or the economic or social wellbeing of the public to be critical electronic record for the purposes of sections 56 to 60.

Registration of critical databases

57. (1) The Minister may by notice in the *Gazette* determine

(a) requirements for the registration of a critical database;

(b) procedures for the registration of a critical database; and

(c) any other matter relating to registration.

(2) Registration of a critical database means recording the following information

(a) the full name, address and contact details of the critical database administrator;

(b) the location of the critical database, including the locations of the component parts where a critical database is not stored at a single location; and

(c) a general description of the categories or types of information stored in the critical database.

Management of critical databases

58. (1) The Minister shall prescribe minimum standards for prohibitions in respect of

(a) the general management of a critical database;

(b) access to, transfer and control of a critical database;

(c) infrastructural or procedural rules and requirements to secure the integrity and authenticity of a critical electronic record;

(d) procedures and technological methods to be used in the storage or archiving of a critical database;

(e) accident recovery plans in the event of loss of critical databases or parts of the database;

(f) the security of the databases;

(g) the physical safety of a person in control of the critical database; and

(h) any other matter required for the adequate protection, management and control of a critical database.

(2) This Act shall not be construed to limit the right of a public body to perform an authorised function in terms of any other law.

Restrictions on disclosure of information

59. (1) Information contained in the register of a critical database shall not be disclosed to another person other than to employees of the Agency who are responsible for the keeping of the register.

(2) The Agency is at liberty to disclose information to

(a) a law enforcement agency; and

(b) a Ministry, Department or Agency.

(3) Nothing in this law shall preclude the Agency from pleading in proceedings relating to information held in its custody or records that production or disclosure of a matter may be prejudicial to the security of the State or injurious to the public interest in accordance with article 135 of Constitution.

Audits

60. (1) The Minister may direct that audits be conducted by the critical database administrator to assess compliance with the provisions of this Act.

(2) For the purposes of subsection (1), the National Information Technology Authority shall act as the critical electronic records and database administrator responsible for overseeing ICT infrastructure of the Republic.

Non-compliance with Act

61. (1) The Minister on receipt of the audit report shall consider,

(a) any action recommended to remedy the non-compliance; and

(b) the period within which the remedial action shall be performed.

(2) The Minister shall report the recommendation to the National Security Council and the Council may take action or give directions that it considers necessary for the protection of national security.

(3) The National Information Technology Authority shall advise the Minister on matters relating to the audit of the ICT infrastructure of the Republic.

Appeal Tribunal

Establishment of the Information Communication Technology Tribunal

62. (1) There is established by this Act an appeal tribunal, known as the Information Communication Technology Tribunal referred to in this Act as "the Tribunal".

(2) The Tribunal shall be convened on an *ad hoc* basis to consider an appeal

(a) against a decision or order made by the Agency;

(b) on a particular matter under a licence.

Composition of the Tribunal

63. (1) The Tribunal consists of

(a) a chairperson who is either a retired Justice of the Superior Court or a lawyer of at least fifteen years standing who has experience in electronic communication law, policy and regulatory matters or arbitration, and

(b) two other members with knowledge of or experience in the information communication technology related matters, industry, electronic engineering, law, economics, business or public administration.

(2) The members of the Tribunal shall be appointed by the Minister.

(3) The Minister shall also appoint a Registrar for the Tribunal for the smooth operations of the Tribunal.

(4) The Registrar and other staff are employees of the Agency.

(5) The expenses of the Tribunal shall be paid out of income derived by the Agency and shall be part of the annual budget of the Agency.

Rules of Procedure of Tribunal

64. The Board shall, propose rules of procedure for the Tribunal.

Appeals against decisions of the Agency

65**.** (1) A person affected by a decision of the Agency may appeal against the decision by notice of appeal to the Tribunal in accordance with the rules of procedure of the Tribunal.

(2) The notice of appeal shall be sent within twenty-eight days after the date the decision is announced or the date of receipt of the decision that is being appealed against.

(3) The notice of appeal shall set out

(a) the decision appealed against;

(b) the provision under which the decision appealed against was taken; and

(c) the grounds of appeal.

(4) After the receipt of a notice of appeal, the Tribunal shall be convened within one month to consider the appeal.

Decision of Tribunal

66. (1) The Tribunal, after hearing the appeal, may

(a) quash the decision;

(b) allow the appeal in whole or in part;

(c) vary the decision of the Agency in any manner and subject to any conditions or limitations it thinks fit but shall not impose any condition or requirement beyond the powers of the Agency under the Act; or

(d) dismiss the appeal and confirm the decision of the Agency.

(2) The Tribunal may take into account a submission filed by any person in reaching a decision on an appeal brought before it.

(3) A decision of the Tribunal shall have the same effect as a judgment of the High Court.

Appeals against the decisions of the Tribunal

67. (1) A decision of the Tribunal may be the subject of an appeal.

(2) An appeal under this section

(a) lies to the Court of Appeal;

(b) shall relate only to a point of law arising from the decision of the Tribunal; and

(c) may be brought only by a party to the proceedings before the Tribunal.

(3) The appeal shall be filed in the Court of Appeal ninety days after the decision of the Tribunal and there shall be no extension of time.

Industry Forum

Establishment of Industry Forum

68. (1) There is hereby established an Industry Forum which shall be a platform to bring the industry together from time to time to discuss matters of common interest that relate to the industry.

(2) The Agency may designate an industry body to be the Forum by notifying that body in writing if the Agency is satisfied that

(a) the membership of the body is open to the relevant parties and is fully representative of the industry;

(b) the body is capable of performing as required under the relevant provisions of this Act; and

(c) the body has the administrative capacity to service the Forum.

(3) The body shall agree in writing to be the Forum, before being designated by the Agency.

(4) Despite the designation, each licensed entity under the Act is deemed to be a member of the Forum.

(5) The Agency may decide that an existing industry body that was previously designated under subsection (2) to be an Industry Forum is no longer an Industry Forum if satisfied that the body does not meet the requirements of this section any longer.

(6) A designation or withdrawal of designation under this section takes effect from the date specified by the Agency.

(7) Until the Agency designates a body, the Agency has the obligation to facilitate the meeting of the industry to perform the functions of the Forum.

(8) The Ministry and the Agency shall participate in the Forum as observers.

Industry code

69. (1) The Forum may prepare a voluntary industry code to deal with a matter provided for in this Act

(a) on its own initiative; or

(b) at the request of the Agency.

(2) The code shall not be effective until it is registered by the Agency.

(3) The Agency shall register a voluntary industry code if it is consistent with

(a) the objects of this Act;

(b) regulations, standards or guidelines made under this Act; and

(c) provisions of this Act which are relevant to the particular matter or activity.

(4) The Agency may refuse to register the code, if the Agency is not satisfied that there has been sufficient opportunity for public consultation in the development of the code by the Forum.

(5) The Agency shall notify the Forum in writing and provide the reasons for the refusal to register the code within thirty days after the refusal.

(6) Where the Agency does not register or refuses to register a voluntary industry code within a period of thirty days after the date that the voluntary industry code was submitted for registration, the Agency is deemed to have refused the registration of the voluntary industry code unless the Industry Forum receives a written notice of registration of the voluntary industry code after that period.

Liability of service providers and intermediaries

Mere conduit

70. (1) An intermediary or service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of electronic records through an information system under its control, as long as the intermediary or service provider

(a) does not initiate the transmission;

(b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection of the electronic record; and

(d) does not modify the electronic record contained in the transmission.

(2) The acts of transmission, routing and provision of access include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than an anticipated recipient; and

(c) for a period no longer than is reasonably necessary for the transmission.

Electronic record transmission

71. An intermediary or service provider who transmits an electronic record provided by a recipient of the service through an information system under its control is not liable for the automatic, intermediate and temporary storage of that electronic record, where the purpose of storing the electronic record is to make the onward transmission of the electronic record more efficient to other recipients of the service on their request, as long as the service provider

(a) does not modify the electronic record;

(b) complies with conditions on access to the electronic record;

(c) complies with rules regarding the updating of the electronic record, specified in a manner widely recognised and used by the industry;

(d) does not interfere with the lawful use of technology widely recognised and used by the industry to obtain information on the use of the electronic record; and

(e) removes or disables access to the electronic record it had stored upon receiving a take-down notice under this Act.

Hosting

72. (1) An intermediary or service provider who provides a service that consists of the storage of electronic records provided to a user of the service, is not liable for damages arising from information stored at the request of the recipient of the service, as long as the service provider

(a) does not have actual knowledge that the information or an activity relating to the information is infringing the rights of a third party,

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the information is apparent or can be reasonably inferred, and

(c) upon receipt of a take-down notification under this Act, takes action expeditiously to remove or to disable access to the information.

(2) The limitations on liability established by this section do not apply to a service provider unless

(a) it has provided an address to receive notifications of infringement; or

(b) it has an agent for receipt of notification of infringement.

Information location tools

73. An intermediary or service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing electronic record or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the intermediary or service provider

(a) does not have actual knowledge that the electronic record or an activity relating to the electronic record is infringing the rights of that person or the State;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic record is apparent or can be reasonably inferred;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes or disables access to the reference or link to the electronic record or activity within a reasonable time after being informed that the electronic record or the activity relating to the electronic record, fringes the rights of a person or the State.

Take-down notification

74. (1) A person who claims that an electronically published matter is illegal or unlawful shall notify the publisher.

(2) A notification of unlawful activity shall be in a permanent medium addressed by the complainant to the intermediary or service provider or its designated agent and shall include

(a) the full names and address of the complainant;
(b) the written or electronic signature of the complainant;
(c) identification of the right that has allegedly been infringed
(d) identification of the material or activity that is claimed to be the subject of unlawful activity;
(e) the remedial action required to be taken by the intermediary or service provider in respect of the complaint; and
(f) telephonic and electronic contact details, if any, of the complainant.

(3) A person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable to pay a pecuniary penalty equivalent to five hundred penalty units.

(4) The intermediary or service provider is liable for wrongful takedown in response to a notification.

Monitoring and compliance

75. (1) An intermediary or service provider shall not be required to monitor an electronic record processed by means of a personal system in order to ascertain whether its processing would constitute or give rise to an offence or give rise to civil liability.

(2) Nothing in this section shall relieve an intermediary or service provider from

(a) an obligation to comply with an order or direction of a Court or other competent Agency; or
(b) any contractual obligation.

Risk Assessments and Mitigation

76. (1) Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) shall conduct annual risk assessments to identify systemic risks associated with their platforms, including but not limited to disinformation, hate speech, child exploitation, and other harmful content.

(2) VLOPs and VLOSEs shall submit risk mitigation plans to the National Information Technology Authority within thirty (30) days following completion of the assessment.

(3) Risk management practices shall be subject to independent third-party audits every two (2) years, and the audit reports shall be submitted to National

Information Technology Authority and made publicly available in accordance with prescribed guidelines.

Transparency Obligations

77. (1) VLOPs, VLOSEs, and Certifying Authorities shall publish biannual transparency reports detailing

(i) content moderation actions undertaken, including removals and account suspensions;

(ii) complaints received and the nature and resolution of such complaints;

(iii) the use of automated tools, including artificial intelligence systems, for filtering or moderating content; and

(iv) algorithmic disclosure, which shall include the criteria used in content ranking, targeted advertising, and recommendation systems.

(2) Certifying Authorities shall also publish annual transparency reports detailing:

(i) the number of digital certificates issued, revoked, or suspended; and

(ii) the reasons and circumstances surrounding such actions.

Protection of Children

78. (1) Service providers offering services directed at or likely to be accessed by childrens shall implement robust age-verification mechanisms to prevent unauthorised access by underage users.

(2) No person or entity shall deliver targeted advertising based on the personal data of childrens, whether directly or through automated profiling systems.

Due diligence obligations

79. A licensee shall conduct periodic risk assessments in accordance with standards prescribed by the National Information Technology Authority, with a view to identifying, managing, and mitigating potential threats to the integrity, confidentiality, and availability of its systems and services.

Limitations and prohibited acts

80. (1) Except as provided in this Act

(a) any person or entity that provides an electronic communication service to the public shall not knowingly divulge the contents of a communication while in electronic storage by that service to any person or entity; and

(b) a person or entity providing remote computing service to the public shall not knowingly divulge the contents of any communication which is carried or maintained on that service to any other person or entity

(i) on behalf of, and received by means of electronic transmission from a subscriber or customer of the service; and

(ii) solely for the purpose of providing storage or computer processing services to the subscriber or customer,

if the provider is not authorised to access the contents of the communications to provide any service other than storage or computer processing.

(2) A person or entity may divulge the contents of a communication

(a) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;

(b) as otherwise authorised by law;

(c) with the lawful consent of the originator, an addressee, intended recipient of the communication, or the subscriber in the case of remote computing service;

(d) to a person employed, authorised or whose facilities are used to forward the communication to its destination;

(e) as may be necessarily incident to the provision of the service or to the protection of the rights or property of the provider of that service; or

(f) to a law enforcement agency if the contents were inadvertently and unintentionally obtained by the service provider and appear to relate to the commission of a crime.

Savings

81. Sections 70 to 80 do not affect

(a) an obligation founded on an agreement;

(b) the obligation of a service provider acting as in that capacity under a licensing or other regulatory regime established by or under any law; and

(c) an obligation imposed by law or by a Court order to remove, block or deny access to an electronic record.

Miscellaneous matters

Territorial scope of offences under this Act

82. (1) This Act has effect in relation to a person of whatever nationality outside as well as within the country and where an offence under this Act is committed by a person in any place outside the country, the person may be dealt with as if the offence had been committed within the country.

(2) This Act shall apply if, for the offence in question

(a) the accused was in the country at the material time;

(b) the electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time;

(c) the electronic payment medium was issued by a financial institution in the country; or

(d) the offence occurred within the country, on board a Ghanaian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence was committed, whether paragraph *(a), (b)* or *(c)* applies.

Guidelines, directives, or codes of practice

83. The National Information Technology Authority may, for the purpose of giving effect to the provisions of this Act, issue guidelines, directives, or codes of practice as it considers necessary for the effective implementation and enforcement of this Act and any Regulations made under it.

Regulations

84. The Minister may by legislative instrument make regulations

(a) to define, enlarge or restrict the meaning of a word or expression used in this Act;

(b) to specify provisions of or requirements under another enactment to which this Act does not apply;

(c) to prescribe records, information or classes of records or information not applicable to this Act;

(d) to prescribe records or classes of records for which a requirement under law for the signature of a person must be satisfied by an electronic signature and proof that, in view of the

circumstances including any relevant agreement and the time the electronic signature was made,

(i) the electronic signature is reliable for the purpose of identifying the person, and

(ii) the association of the electronic signature with the relevant electronic record is reliable for the purposes for which the electronic record was made;

(e) to provide for electronic signatures;

(f) to provide for the electronic means to be used to send, receive or retain information or records in electronic form if an enactment requires a person to send, receive or retain the information or records; and

(g) to provide for any other matter necessary for the effective implementation of this Act.

Interpretation

85. In this Act, unless the context otherwise requires,

"access" includes the actions of a person who, after taking note of data, becomes aware of the fact that there is no authorisation to access that data and still continues to access that data;

"addressee", in respect of an electronic record, means a person who is intended by the originator to receive the electronic record, but not a person acting as an intermediary with respect to that electronic record;

"Agency" means the National Information Technology Agency;

"algorithmic disclosure" means the obligation of a platform or service provider to make available meaningful information about the logic, significance, parameters, and potential impact of algorithms used in ranking, recommending, or filtering content or advertisements;

"authentication products or services**"** means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider**"** means a person whose authentication products or services have been accredited by the Certifying Agency under this Act;

"automated profiling**"** means the use of automated processing techniques, including artificial intelligence or machine learning, to analyse personal data in order to evaluate certain aspects of a person, in particular to predict or assess behaviour, preferences, interests, or location;

"automated transaction**"** means an electronic transaction conducted or performed, in whole or in part, by means of electronic records in which the conduct or electronic records of one or both parties are not reviewed by an individual in the ordinary course of the individual's business or employment;

"Biometric authentication**"** means the process of verifying an individual's identity based on measurable physiological or behavioural characteristics, including but not limited to fingerprints, facial features, voice patterns, retinal scans, or other biometric identifiers, used in connection with electronic identification or digital signatures;

"Board" means Board of the Agency;

"browser" means a computer programme which allows a person to read hyperlinked electronic records;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;

"ccTLD" means country code domain at the top level of the Internet's domain name system assigned according to the two-letter codes in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision);

"Certificate practice statement" means a statement published by a certification service provider that outlines the practices, procedures, and security controls used in the issuance, management, revocation, and renewal of digital certificates;

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with an electronic record;

"Certifying Agency" means the Certifying Agency established under this Act;

"clear days" means complete days excluding the day of dispatch;

"computer" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function but does not include
(a) portable hand held calculator;
(b) an automated typewriter or typesetter;
(c) a similar device which is non-programmable or which does not contain any data storage facility; or
(d) any other device that the Minister may prescribe in the Gazette;

"computer output" **or "**output" means a statement or representation, whether in written, printed, pictorial, graphical, electronic, digital or any other form, purporting to be a statement or representation of fact
(a) produced by a computer; or
(b) accurately translated from a statement or representation so produced;

"computer service" includes computer time, computer output, data processing and the storage or retrieval of a programme or data;

"consumer" means an individual person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"controller" means a person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"Court" means any judicial, quasi-judicial or other administrative tribunal established by law;

"critical database" means a crucial set of data in an electronic record related to national security or the economic well-being of the public determined by the Minister;

"critical database administrator" means the person responsible for the management and control of a critical database;

"critical electronic record" means an electronic record, group or classification of electronic record which is declared by the Minister to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens;

"cyber inspector" means a staff of the National Information Technology Agency with power to monitor, investigate, prosecute any offence under this Act and any other law enforcement agency acting under any provision of this Act;

"damage" includes impairment to a computer or the integrity or availability of a programme or data held in a computer that:
(a) causes loss within the period prescribed under the Limitation Decree, 1972 (N.R.C.D. 54),
(b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of a person,
(c) causes or threatens physical injury or death to a person, or
(d) threatens the public interest;

"decryption information" means information or technology that enables a person to readily retransform or unscramble an encrypted programme or data from its unreadable and incomprehensible format to its plain text version;

"device" means any thing or apparatus that is used or capable of being used to intercept a function of a computer or electronic record;

"digital platform" means an online-based system or interface, including web-based platforms and app-based ecosystems, that facilitates interaction between users for the exchange of goods, services, information, or content, including social media platforms, online marketplaces, and digital service aggregators;

"digital signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

"domain name system" means a system to translate domain names into IP addresses or other information;

"E-Gazette" means an official Government publication issued in electronic format, which is accessible online, authenticated by electronic or digital signature, and which carries the same legal effect and admissibility in court as the print version of the Gazette;

"e-government services" means a public service provided by electronic means by a public body in the country;

"e-mail" means electronic mail, an electronic record used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"electronic agent" means a computer programme or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of electronic records;

"electronic payment medium" includes any medium issued to a holder capable of being used to make an electronic financial transaction;

"electronic record" includes data generated, sent, received or stored by electronic means:
(a) voice, where voice is used in an automated transaction; and
(b) a stored record;

"electronic signature" means any data in electronic form, affixed to or logically associated with a data message, which is used by a person to indicate their agreement to the content of that data message or transaction, and which

is capable of identifying the signatory and maintaining the integrity of the signed information;

"electronic transaction" means a transaction by an electronic agent;

"encrypted product" means a product that makes use of encryption techniques and is used by a sender or recipient of electronic record to ensure
(a) that the data can be accessed only by relevant persons,
(b) the authenticity of the data,
(c) the integrity of the data, or
(d) that the source of the data can be correctly ascertained;

"encrypted programme or electronic record" means a programme or data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilized for the transformation or scrambling and irrespective of the medium in which the programme or data occurs or can be found for the purposes of protecting the content of the programme or data;

"encryption provider" means any person who provides or who proposes to provide encryption services or products in the country;

"encryption service" means a service which is provided to a sender or a recipient of an electronic record or to anyone storing an electronic record, which is designed to facilitate the use of encryption techniques to ensure
(a) that the data or electronic record can be accessed or can be put into an intelligible form only by certain persons,
(b) that the authenticity or integrity of the data or electronic record is capable of being ascertained,
(c) the integrity of the data or electronic record, or
(d) that the source of the data or electronic record can be correctly ascertained;

"essential emergency service" means a vital service to avoid the imminent occurrence of a situation which is out of the ordinary which threatens to endanger a person, public safety or cause damage to property;

"financial institution" means an entity that undertakes financial intermediation;

"financial intermediation" means a process of transferring funds from one entity to another entity;

"Forum" means Industry Forum;

"function" includes logic, control, arithmetic, deletion, storage and retrieval, and communication or telecommunication to, from or within a computer;

"Gazette" includes an electronic record of the Gazette and publication on the website of the appropriate Government Agency;

".gh domain name space" means the .gh ccTLD assigned to the Republic according to the two-letter codes in the International Standard ISO 3166;

"Government" means any authority by which the executive authority of the Republic is duly exercised;

"home page" means the primary entry point webpage of a website;

"hyperlink" means a reference or link from some point in one electronic record directing a browser or other technology or functionality to another electronic record or point in that electronic record or to another place in the same electronic record;

"hyper text" means a reference or link from some point in one electronic record directing a browser or other technology or functionality to another electronic record or point or to another place in the same electronic record;

"incorporated body" means an entity registered under the Companies Act 2019 (Act 992), the Incorporated Private Partnerships Act 1962 (Act 152) or the Trustees Incorporation Act, 1962 (Act 106);

"incident response plan" means a formal set of procedures established by a licensed entity or certifying authority for detecting, reporting, responding to, and recovering from cybersecurity incidents or breaches that affect the integrity, availability, or confidentiality of its systems or services;

"industry" means the communications industry;

"Industry Forum" means the communications industry meeting from time to time to discuss matters of common interest to and concerning the industry;

"information system" includes a system for generating, sending, receiving, storing, displaying or otherwise processing electronic records and the Internet;

"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of electronic records between or among points specified by a user and the processing and storage of data at the individual request of the recipient of the service;

"intercept" includes, in relation to a function of a computer or electronic record, listening to or recording a function of a computer or electronic record, or acquiring the substance, meaning or purport of it;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular electronic record or provides other services with respect to that electronic record;

"interoperability standards" means technical specifications that ensure digital systems, applications, and processes are capable of exchanging and using information securely, effectively, and consistently across different platforms, jurisdictions, or certifying authorities;

"Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and future versions of the interconnected system;

"IP address" means the number identifying the point of connection of a computer or other device to the internet;

"law enforcement agency" means the police, customs, excise and preventive service and any other law enforcement agency authorised by law to exercise police powers;

"Minister" means the Minister responsible for Communications;

"Ministry" means the Ministry responsible for Communications;

"notice" means transactional message or notification intended to elicit the subscriber's choice to opt-in or opt-out of a service, or an emergency communication prescribed by law;

"originator" means a person by whom, or on whose behalf, an electronic record purports to have been sent or generated prior to storage, but does not mean a person acting as an intermediary with respect to that electronic record;

"person" includes a public agency;

"personal information" means information about an identifiable individual, including, but not limited to:
(a) information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being; disability, religion, conscience, belief, culture, language and birth of the individual;
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
(c) any identifying number, symbol, or other particular assigned to the individual;
(d) the address, fingerprints or blood type of the individual;
(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of original correspondence;
(g) the views or opinions of another individual about the individual;
(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would

reveal information about the individual, but excludes information about an individual who has been dead for more than twenty years;

"plain text version" means a programme or original data before it has been transformed or scrambled to an unreadable or incomprehensible format;

"prescribe" means prescribe by directive, notice or Regulation under this Act;

"programme or computer programme" means data representing instructions or statements which when executed in a computer, causes the computer to perform a function;

"programme or data" includes a reference to a programme or data held in any removable storage medium which is for the time being in the computer;

"public agency" means a body set-up by Government in the public interest with or without an Act of Parliament;
(a) department of central government or a department in local government; or
(b) any other functionary or institution when
    (i) exercising a power or discharging a duty in terms of the Constitution; or
    (ii) exercising a power or performing a function in terms of any legislation;

"public interest" includes a right or advantage which enures or is intended to enure to the general benefit of the people of this country, including but not limited to access to essential digital services, protection of personal data, promotion of cybersecurity, and the safeguarding of national digital infrastructure;

"public key" means the key which is available to the public for purposes of the encryption of an electronic key which is linked to a private decryption key held exclusively by the issuer of the key available to the public;

"Public Key Infrastructure" (PKI) means a system of policies, roles, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and public keys, enabling secure electronic transactions and communication through authentication, confidentiality, integrity, and non-repudiation;

"Qualified Electronic Signature" means an electronic signature that—
(a) is uniquely linked to the signatory;
(b) is capable of identifying the signatory;
(c) is created using means that the signatory can maintain under their sole control; and
(d) is based on a qualified certificate issued by a certification service provider accredited or recognised under this Act;

"recommendation system" means an automated system used by an online platform to suggest content, products, services, or interactions to users based on data collected from or about those users or other users;

"repository" means the primary register of electronic records or information maintained by a registry or certification service provider, for the purpose of storing, publishing, or retrieving digital certificates, public keys, or related transactional data;

"risk management practices" means structured processes, tools, and procedures employed to assess, monitor, and address operational, technological, legal, and reputational risks within an electronic communication environment;

"risk mitigation plan" means a documented strategy developed by a service provider or platform to identify, reduce, and manage potential systemic risks and vulnerabilities associated with its operations, systems, or content dissemination processes;

"Root CA" means the Root Certification Authority, being the top-level trusted entity in a Public Key Infrastructure that issues and digitally signs certificates for subordinate certification authorities, and serves as the foundational trust anchor for the validation of all digital certificates issued under the infrastructure;

"second level domain" means the sub domain immediately following the ccTLD;

"security agency" means a body connected with national security;

"service provider" means any person providing information system services;

"statutory provision" means by or under an Act of Parliament;

"sub domain" means any subdivision of the .gh domain name space which is the second level domain;

"Subscriber" means a person or entity that is the subject named or identified in a digital certificate, who has applied for and been issued the certificate by a certification service provider, and who holds the corresponding private key associated with the public key listed in the certificate;

"TCP/IP" means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet;

"TI-D" means a top level domain of the domain name system;

"third party" in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems;

"transaction" means a transaction of either a commercial or non-commercial nature and the provision of information and e-government services;

"transparency report" means a periodic report published by a service provider, certifying authority, or platform detailing the scope and nature of content moderation activities, use of automated tools, algorithmic processes, complaints received and resolved, and other operational metrics as required under this Act;

"unauthorised access" is access of any kind by a person to a programme or data held in a computer without authority if:
(a) the person is not personally entitled to control access of the kind in question to the programme or data; and
(b) the person does not have consent to access the kind of programme or data from the person who is entitled to control access;

"unincorporated body" means an entity registered under the Registration of Business Names Act, 1962 (Act 151) or any person carrying on business without a registration or without a certificate of incorporation;

"universal access" means access by all citizens of Ghana to internet connectivity and electronic transactions;

"user-generated content" means any form of content, including text, images, videos, or audio, created and uploaded by a user of an online platform, which is not pre-selected or controlled by the service provider other than through moderation or algorithmic curation;

"Very Large Online Platforms" or "VLOPs" means online platforms that provide intermediary services primarily consisting of hosting user-generated content, which reach an average of forty-five million or more monthly active users within the jurisdiction or relevant region, and which, due to their size, have a significant societal or systemic impact on the dissemination of information, public discourse, or access to goods and services online;

"Very Large Online Search Engines" or "VLOSEs" means online search engines that allow users to input queries to retrieve information from websites across the internet, and which reach an average of forty-five million or more monthly active users, thereby having a considerable effect on the visibility of online information and the flow of digital traffic;

"webpage" means an electronic record on the World Wide Web;

"website" means a location on the Internet containing a home page or web page; and

"World Wide Web" means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer.

Repeals and savings

86. (1) The Electronic Transactions Act, 2008 (Act 772) is hereby repealed.

(2) Despite the repeal under subsection (1), any licence, authorisation, notice, or other lawful act issued or done under the repealed enactment, and in force immediately before the coming into force of this Act, shall, to the extent that it is not inconsistent with this Act, be deemed to have been issued or done under this Act and shall continue in force until it is revoked, reviewed, cancelled, terminated, or expires.
(3) The Act shall not affect the repealed enactment in the operation of offences committed, penalties imposed or proceedings commenced before the coming into force of this Act.

Modification of existing enactments
87. (1) The provisions of any enactment relevant to this Act and in existence before the coming into force of this Act shall have effect subject to such modifications necessary to give effect to this Act.
(2) Where there is a conflict or inconsistency between the provisions of this Act and any other enactment relevant to this Act, the provisions of this Act shall prevail.

Transitional Provisions
88. (1) A licence, frequency authorisation, permit or certificate issued by the National Communications Authority in respect of electronic communications, spectrum, or broadcasting services shall remain valid until it is revoked, cancelled, terminated by the Authority, or expires in accordance with its terms.
(2) Licensees and entities subject to new obligations under this Act shall be given a period of twelve months from the commencement of this Act, or such longer period as may be prescribed by the Minister, to bring their operations into full compliance.

**Date of Gazette notification:*