General Legal Framework for Electronic Commerce and Electronic Signatures

Electronic commerce (*e-commerce*) plays a key role in economic growth and development. It reduces transaction costs for companies, consumers and public administrations, broadens the geographical scope in which products and services can be bought and sold and, through *online* transactions, significantly increases the range of products and services available.

Indeed, e-commerce requires an effective and comprehensive legal framework in order to develop in a global, multilateral, interconnected and evolving world.

Thus, the aim of this decree-law is to provide Timor-Leste with a legal framework that promotes the development of electronic commercial transactions within the broader framework of the information society, offering significant opportunities for investment and employment while stimulating economic growth and innovation.

To this end, in drafting this decree-law, the opportunity has been taken to enshrine some underlying issues, outside the scope of commercial transactions, which are considered necessary to ensure the effectiveness of this legislative initiative, namely the provisions governing the validity of contracts concluded electronically, the use of electronic records and the legal status of electronic signatures.
In this sense, the function of assessing and certifying the conformity of electronic signature products used in the provision of electronic signature services is entrusted to a certification body. Accordingly, in order to ensure better and greater oversight of these entities by holders and third parties, it was decided to create a register with the accrediting authority, which, although merely declaratory in nature, is compulsory for certifying entities that issue certificates.

Thus, electronic signatures issued by an accredited certification body have the probative force of a signed private document and can be used as evidence under the general terms of the law.

A supervisory body for e-signature and e-commerce is also established, whose functions are entrusted to the Information and Communication Technologies Agency I.P. (TIC TIMOR), including the investigation of administrative offenses, which are foreseen, and the imposition of the respective fines, in the event of infractions.

To this end, a system of penalties has been established for infringements in the field of electronic signatures and commerce, with fines set within very broad frameworks, so that they can be applied to the various situations that arise, and are a deterrent.

Among other things, this law establishes legal equivalence between *online* and paper-based transactions, covering transactions in both the public and private sectors.
Likewise, the requirements governing *online* transactions are established, including the specification of the information to be provided to consumers by e-commerce providers, adopting the principle of technological neutrality with regard to electronic signatures and records.

In addition, this law defines the requirements for the execution and acceptance of electronic contracts and records, and the possibility of using electronic signatures.

It also lays down rules on the use of unsolicited commercial e-mail, commonly known as "*spam*", defines and prohibits the use of fraudulent e-mail and provides for a mechanism and jurisdiction for resolving disputes relating to *online* commercial transactions.

On the other hand, this law establishes the principle of non-discrimination between national and foreign electronic signatures and registrations, recognizes the legitimacy of foreign electronic signatures and registrations in Timor-Leste and, in doing so, aims to facilitate international trade.
Finally, the aim of this law is also to allow the use of out-of-court dispute resolution for conflicts arising in this area, without the general legislation impeding the resolution of these disputes electronically.

As recognized in the National Policy for Information and Communication Technologies (ICT), the aim of this law is to facilitate the interaction and involvement of citizens and companies with the Public Administration, both in national and international issues in the field of e-commerce.

It should be noted that this Decree-Law also aims to encourage the development of paperless cross-border trade, thus supporting greater integration of Timor-Leste into the regional and global economy. In this sense, it is essential that cooperation mechanisms are created with other countries to facilitate and encourage the use of e-commerce.

Furthermore, this law seeks to reflect the best international practices in this area, approximating, among others, the Model Law of the United Nations Commission on International Trade Law (UNCITRAL) on Electronic Commerce, the Law of the United Nations Commission on International Trade Law (UNCITRAL) on Electronic Commerce and the Law of the United Nations Commission on International Trade Law (UNCITRAL) on Electronic Commerce.
UNCITRAL Model Law on Electronic Signatures and the UNCITRAL Model Law on Transferable Electronic Records.

Finally, it should be noted that this decree-law is neutral from a technological point of view, on the assumption that technology has the ability to develop continuously and, as such, solutions are devised that involve applying the options set out in it in a flexible way that allows new technologies to be used in a way that is appropriate and consistent with the objectives of facilitating commercial transactions and the fluidity of economic development.

Accordingly, the Government hereby decrees, pursuant to Article 115 (1) (e) and (o) and Article 116 (d) of the Constitution, to be valid as law, as follows:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object

This decree-law establishes the general legal framework applicable to electronic transactions, records and signatures, as well as their use, in particular in the field of electronic commerce.

Article 2

Scope

1. This statute shall apply to any natural or legal person who sells or offers to sell any services or goods through electronic commerce to any natural or legal person domiciled, headquartered or established in Timor-Leste.

2. The provisions of this Decree-Law shall also apply to the conclusion and acceptance of electronic records, the use and legal status of electronic signatures and the conclusion of contracts by electronic means, whether or not they refer to electronic commerce, whenever the law of Timor-Leste is chosen by the parties or is otherwise deemed applicable.

3. This Decree-Law is without prejudice to the application of compatible legislation in force, in particular the related provisions in the fields of telecommunications services, trade and customs, data protection and consumer protection that result from other applicable national legislation.

Article 3
Exclusions from scope

Unless the use of electronic records and communications meets the special legal requirements of authenticity, this Decree-Law shall not apply to the following acts:

a) Wills and other acts of inheritance law;
b) Marriage, adoption, divorce and other family law acts;
c) The transfer of real estate and any real estate matters requiring notarial intervention;
d) Any other documents whose validity depends on notarial intervention;
e) Procedural acts of justice, including orders or notifications from judicial authorities;
f) Notification of cancellation or termination of public utility services;
g) Default, acceleration, repossession, foreclosure or eviction, or the right to relief under a credit agreement secured by a lease of an individual's principal residence or an individual's primary residence;
h) Cancellation or termination of health insurance or life insurance benefits;
i) Securities, such as shares and bonds, and other investment instruments;
j) Recall of a product or notice of material failure of a product that could endanger health or safety.

Article 4
Definitions

For the purposes of this decree-law, the following definitions apply:

a) "recipient" means the person whom the author wishes to receive the electronic communication, but does not include the person who acts as an intermediary in relation to that electronic communication;
b) "automated electronic system" means a computer program or electronic or other automated means used to initiate an action or to respond to data messages or performances, in whole or in part, without review or intervention by a person when an action is initiated or a response is generated by the system;
c) "Bill of exchange" means an unconditional written order, signed and dated, by which the drawer orders the drawee to pay a specified sum of money to the beneficiary or to his order, on demand or at another specified time;
d) "bill of lading" means a commercial document, bearing a unique number, required for the movement of all goods across customs borders, which serves as proof of the conditions of carriage agreed between the importer and the supplier;

e) "certificate" means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of a person holding a particular key pair;
f) "certifying entity" means a public or private entity competent to issue a certificate, as well as assess and certify the conformity of electronic signature processes, systems and products with the technical requirements set out in this law;
e) "Accreditation authority" means the public body responsible for accrediting and supervising certification bodies;
g) "commercial electronic mail message" means a statement or information sent by electronic mail the primary purpose of which is the advertising or promotion of a commercial product or service, not including an electronic mail message relating to an order for a product or service of the sender generated by the recipient of the electronic mail message;
h) "communications" means any statement, demand, notice or request, including an offer and the acceptance of an offer, which the parties are required to make or choose to make in connection with the formation or performance of a contract;
i) "consumer" means any natural or legal person to whom goods or services are supplied for non-business use by a person pursuing an economic activity in a business capacity with a view to obtaining benefits;
j) "data message" means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including but not limited to electronic data interchange, electronic mail, electronic messages, telegram, telex or fax;
k) "electronic commerce" or *"e-commerce"* means an activity involving the purchase, sale, rental or exchange of goods or services, by consumers, businesses and public services, in the national territory or in a cross-border transaction, where such activities are transacted or facilitated by means of electronic communications, including, in particular, financial transactions carried out through electronic data exchanges, including "mobile commerce" or "*m-commerce",* as defined in this statute;
l) "electronic communication" means any communication that the parties to an electronic commercial transaction carry out by means of data messages or electronic networks;
m) "e-commerce merchant" means any natural or legal person engaged in commerce in Timor-Leste who offers services or goods for sale, lease or exchange to customers, including public entities, in Timor-Leste or in another country, through an electronic transaction, including also any natural or legal person outside Timor-Leste who offers services and/or goods for sale, lease or exchange to customers in Timor-Leste without the intervention of any intermediary;
n) "electronic data interchange" means the transfer of data between two computer systems in a standardized electronic format, without human intervention;
o) "Electronic record" means a record made, communicated, received, stored or processed in an electronic system or in any system or device used for transmission from one electronic system to another;
p) "electronic signature" means an electronic sound, symbol or process used to identify a person and indicate his or her approval and intention to be bound by a contract or information;
q) "transferable electronic record" means an electronic record that meets all the requirements set out in Chapter IV of this Decree-Law;
r) "public entity" means any service of the Direct, Indirect or Autonomous Administration of the State, which carries out the functions provided for in Article 17(1).
s) "information" means a description of fact in the form of a document, signature, seal, data, text, images, sound or voice;

t) "information system" means a system for producing, sending, receiving, storing, displaying or otherwise processing electronic communications or information;
u) "intermediary" means a natural or legal person who, on behalf of another natural or legal person, sends, receives or stores, on a temporary or permanent basis, electronic communication or provides other services related to electronic communication, but is not the originator of the content that is sent, received or stored;
v) "key pair" means public and private digital keys that are used to verify the identity of a holder of a digital or electronic transaction;
y) "mobile commerce" or "*m-commerce*" means the use of portable wireless devices, such as cell phones, to conduct electronic commerce and includes the use of such devices to conduct *online* financial transactions.
z) "place of business" means any place where a party maintains a permanent establishment for the purpose of carrying on an economic activity other than the temporary supply of goods or services;
aa) "Promissory note" means a written, signed and dated unconditional promise by which the author undertakes to pay a certain sum of money to the beneficiary or to his order, payable on demand or at another specified time.
bb) "Sender" means the person or entity by whom or on whose behalf the electronic communication is sent or generated prior to storage, where applicable, excluding any intermediary acting in that electronic communication.
cc) "secure electronic signature" means an electronic signature which has been confirmed by technological means, such as a public key infrastructure (PKI) certificate, as being unique to the person using it and which meets the other requirements of this Decree-Law relating to such signatures.
dd) "Holder" means the natural or legal person who holds signature certification data and who acts in his or her own name or on behalf of the person he or she represents.
ee) "*Spam*", unsolicited commercial e-mail.
ff) "transferable document or instrument" means a document or instrument issued on paper which confers on its holder the right to demand performance of the obligation stated therein and to transfer the right to perform the stated obligation by transferring that document or instrument, in particular:
    i. Bills of exchange;
    ii. Bill of lading;
    iii. Promissory note.

Article 5
Principle of national jurisdiction

By virtue of an activity purposely aimed at marketing and selling services and goods in Timor-Leste, any natural or legal person is deemed to be doing business in Timor-Leste and subject to its jurisdiction, whether or not that natural or legal person has a physical or legal presence in the national territory.

Article 6
Effectiveness and non-discrimination

1. The legal effectiveness of an electronic record, an electronic certificate, an electronic signature or a transferable electronic record shall be determined on the basis of its reliability in accordance with the following Article.

2. The provisions of the preceding paragraph shall apply irrespective of:

a) the geographical location where the certificate is issued or the electronic signature, electronic record or transferable electronic record is created or used; or
b) Geographical location of the sender's, owner's, creator's or user's place of business.

3 A certificate issued or used abroad has the same legal effect in Timor-Leste as a certificate issued in national territory, if it offers a substantially equivalent level of reliability.

4 An electronic signature created or used abroad has the same legal effect in Timor-Leste as an electronic signature created or used in the national territory, if it offers a substantially equivalent level of reliability.

5 An electronic record issued or used abroad has the same effect in Timor-Leste as an electronic record created or used in Timor-Leste as an electronic record created or used in the national territory, if it offers a substantially equivalent level of reliability.

6 A transferable electronic record issued or used abroad has the same effect in Timor-Leste as a transferable electronic record created or used in the national territory, if it offers a substantially equivalent level of reliability.

7 In determining whether an electronic record, an electronic certificate or signature or a transferable electronic record offers a substantially equivalent level of reliability, due account shall be taken of recognized international standards.

(8) Notwithstanding the provisions of this Article, where the parties agree between themselves on the use of certain types of electronic signatures or certificates, electronic records or transferable electronic records, such agreement shall be deemed sufficient for the purposes of cross-border recognition, unless such agreement is not valid or effective under the applicable law.

Article 7
Reliability

Where this Decree-Law imposes a reliability requirement, the method for measuring that requirement for an electronic record, certificate or electronic signature, or a transferable electronic record, shall be:

a) As reliable as appropriate for fulfilling the purpose or function for which the method is used, in the light of all relevant circumstances, which may include, but are not limited to, the following assumptions:
   i. Any operational rules relevant to the assessment of reliability;
   ii. Ensuring data integrity;
   iii. The ability to prevent unauthorized access to and use of the system;
   iv. *Hardware* and *software* security;
   v. The regularity and extent of the audit carried out by an independent body;
   vi. The existence of a declaration from a supervisory body, an accreditation body or a voluntary scheme concerning the reliability of the method;
   vii. Any relevant agreement;
   viii. Any applicable industry standard;
   ix. Compliance with recognized international standards.

b) Proof of fulfilment of the function, alone or in conjunction with other evidence.

Article 8
Place of activity

1 For the purposes of this decree-law, a site is not a place of business simply because it is:
a) the location of the equipment and technology supporting an information system used by a party in connection with transferable electronic records;

b) Place where the information system can be accessed by other parties.

2 The mere fact that a person uses an e-mail address or other element of an information system linked to a specific country does not create a presumption that their place of business is in that country.

Article 9
Information requirements

Nothing in this Decree-Law shall affect the application of any legal rule requiring a person to disclose his or her identity, place of business or other information, nor shall it exempt a person from the legal consequences of making inaccurate, incomplete or false statements in this regard.

CHAPTER II
ELECTRONIC RECORDS AND SIGNATURES

Article 10
Freedom to use electronic records

1. No one is obliged to use, provide or accept information in electronic form without their consent.
2. The provisions of this decree-law apply only to transactions in which each party to a deal has agreed that they will be carried out by electronic means.
3. The agreement may be expressly stated by the parties, but may also be determined by the context and circumstances, including the behavior of the parties in the transaction.

(4) The parties to a written contract shall not be obliged to use electronic means by virtue of a provision of that contract, unless this requirement is clearly indicated in letters larger than those contained in the rest of the contract and is expressly agreed by the parties.

5 The agreement to carry out a transaction by electronic means does not oblige either party to carry out any other transaction by electronic means, and either party may refuse to do so.

6. The parties to a transaction may, by agreement, impose additional requirements as to the form or authentication of the contract or transaction in addition to those specified in this Decree-Law.

Article 11
Validity and probative force of electronic records

1. A data message satisfies the legal requirement of written form when its content can be represented as a written statement.

2. Without prejudice to the provisions of any legal provision, rule or regulation, an electronic document, record or signature may not be denied legal effect, including its use as evidence in legal proceedings, or its enforceability, simply because it is electronic:
   a) In electronic format or in an electronic communication;
   b) Referred to in an electronic communication intended to have that legal effect.

3. Where the law requires information to be submitted in writing or provides for certain consequences if such information is not submitted in writing, an electronic record satisfies that legal requirement if the information it contains is accessible in such a way that it can be used for later reference.

Article 12
Retention of electronic records

1. Where a law requires the retention of certain documents, records or information, that requirement shall be satisfied by retention in the form of an electronic record if the following conditions are met:
   a) The information it contains remains accessible so that it can be used for later reference;
   b) The electronic record is kept in the format in which it was originally generated, sent or received, or in a format that can demonstrate that it accurately represents the information originally generated, sent or received;
   c) Where appropriate, information is kept that makes it possible to identify the origin and destination of an electronic record, as well as the date and time it was sent or received.

2. The obligation to retain documents, records or information pursuant to paragraph (1) shall not extend to information generated necessarily and automatically solely to enable a record to be sent or received.

3. Nothing in this Article shall apply:
   a) Overrides any law that expressly provides for the retention of documents, records or information in the form of electronic records;
   b) Prevents any public body from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of its service.

Article 13
Original documents

(1) Where there is a legal requirement that a document, record or information be produced or retained in its original form, or which provides for certain consequences if it is not, that requirement shall be met by producing or retaining the document, record or information in the form of an electronic record, where appropriate:
   a) There is a reliable guarantee as to the integrity of the information as soon as it has been generated for the first time in its definitive form, either as a written document or as an electronic record;
   b) It is required to be presented or shown to the person to whom it is to be presented.

(2) For the purposes of point (a) of the preceding paragraph, the integrity assessment criteria are whether the information has remained complete and unaltered, with the exception of any irrelevant changes arising in the normal course of communication, storage and display, as well as compliance with the reliability standard set out in Article 7.

Article 14
Electronic signatures

(1) Where a law requires a signature or provides for certain consequences if a document or record is not signed, or if the parties to a transaction agree that an electronic signature is required, the requirement is satisfied in relation to the electronic record by an electronic signature, if:
   a) a method is used to identify the person and indicate that person's intention with regard to the information contained in the electronic record;
   b) the method used is determined to be reliable in accordance with the standards specified in Article 7.

2. Where a law requires or the parties to a transaction specify that a secure electronic signature be used, that requirement is satisfied if it can be verified that an electronic signature at the time it was executed is secure:
   a) Unique to the person using it;
   b) Able to identify that person;
   c) Created in a way or using a medium under the exclusive control of the person using it;
   d) Linked to the electronic record to which it refers, in such a way that if the record is changed, the electronic signature is considered invalid.

3. In the verification referred to in the preceding paragraph, any reasonable method may be used, including, in particular, a certificate issued in accordance with the procedures specified in this Ordinance or a commercially reasonable security procedure agreed upon by the parties involved.

4 Unless otherwise agreed between the parties, no provision of this Decree-Law shall be applied in such a way as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that meets the requirements set out in paragraphs 1 and 2.

Article 15
Private agreements

Without prejudice to Article 6, where the parties agree between themselves to use certain types of electronic signatures or certificates, that agreement shall be deemed sufficient for the purposes of cross-border recognition, unless that agreement is not valid or effective under the applicable law.

Article 16
Use of electronic records and signatures by public bodies

1. The law may allow any public body to process certain acts or procedures by means of electronic records or in electronic format, in particular when:
   a) Accepts registration or the submission of documents or information;
   b) Require the creation or storage of documents or other information;
   c) Demand that documents, records or information be provided or kept in their original form;
   (d) issue any authorization, license or approval; or
   e) Issue a prescribed form for a request or notification or other transaction with the public body;
   f) Demand payment of any fee, charge, tax or other amount by any method or form of payment.

2. Whenever, by law, a public body is permitted to carry out any of the functions provided for in paragraph 1 through electronic records or in electronic format, it must, through one or more means that guarantee easy access by the interested public, including, among others, publication in the Official Gazette and on its official website, provide the following information:
   (a) the form and format in which electronic records are to be presented, created, stored, issued or supplied;
   (b) where electronic records are to be signed, the type of electronic signature required, namely a secure electronic signature or the specific type of secure electronic signature;
   (c) the form and format in which that signature is to be affixed to the electronic record and the identity or criteria to be met by any provider of specific security procedures used by the person filing the document;

(d) adequate control processes and procedures to ensure the appropriate integrity, security and confidentiality of electronic records or payments;
e) Any other procedures required for electronic registrations or payments.

(3) Where a natural or legal person is required by law to execute, file, create, retain, display or provide any of the documents, records or applications provided for in paragraph (1) and performs those actions by means of an electronic record or document or with an electronic signature, they shall be presented in the manner and according to the requirements provided for in paragraph (2).

(4) The provisions of this article shall not require any public body to accept or issue any document or information in the form of electronic records or to accept any payment in electronic form.

CHAPTER III
CERTIFICATION OF ELECTRONIC SIGNATURES

SECTION I
CERTIFICATION

SUBSECTION I
ACCESS TO CERTIFICATION ACTIVITY

Article 17
Free access to certification activity

1. It is free to exercise the activity of certification body, and it is optional to apply for the accreditation regulated in article 20 et seq.

2. Without prejudice to the provisions of the previous paragraph, certifying entities that issue certificates must register with the accrediting authority, under the terms to be established by a joint ministerial decree issued by the members of the Government responsible for Trade and Communications.

3. Accreditation and the respective registration are subject to the payment of fees based on the costs associated with the corresponding administrative, technical, operational and inspection tasks, under the terms to be established by a joint ministerial decree of the members of the Government responsible for the areas of Communications and Finance, and constitute revenue for the accrediting authority.

Article 18
Free choice of certification body

1. The choice of certification body is free.

2. The choice of a specific entity cannot be a condition of an offer or the conclusion of any legal transaction.

Article 19
Competent body for accreditation

The accreditation of certification bodies for the purposes of this law is the responsibility of the accrediting authority.

Article 20
Accreditation of the certification body

1. Accreditation of digital signature certification bodies is granted, upon application to the accrediting authority, to bodies that meet the following requirements:
   a) Have adequate capital and financial means;
   b) Provide guarantees of absolute integrity and independence when carrying out the activity of certifying digital signatures;
   c) They have the technical and human resources to meet the safety and efficiency standards laid down in the regulations referred to in Article 33;
   d) Maintain a valid insurance contract to adequately cover civil liability arising from the certification activity.

2. The accreditation is valid for three years and may be renewed for equal periods.

Article 21
Application for accreditation

1. The application for accreditation as an electronic signature certification body must be accompanied by the following documents:
   a) Articles of association of the legal person and, in the case of a company, articles of association;
   b) In the case of a company, a list of all shareholders, specifying their respective holdings, as well as the members of the management and supervisory bodies, and, in the case of a public limited company, a list of all shareholders with significant direct or indirect holdings;
   c) Declarations signed by all natural and legal persons referred to in Article 23(1) that they are not in any of the situations that indicate a lack of good repute referred to in the respective paragraph 2;
   d) Proof of the assets and financial means available and, in particular, in the case of a company, full payment of the share capital;
   e) Description of the internal organization and security plan;
   f) Demonstration of conformity of electronic signature products issued by a recognized certification body accredited under the terms of article 53;
   g) Appointment of the security auditor;
   h) General program of activities planned for the first three years;
   i) A general description of the activities carried out over the last three years or the time elapsed since incorporation, whichever is shorter, and the balance sheet and accounts for the corresponding financial years;
   j) Proof of a valid insurance contract to adequately cover civil liability arising from the certification activity.

2. If the legal person is not incorporated at the time of the application, the application shall be accompanied by the following documents instead of those provided for in point a) of the previous paragraph:
   a) Minutes of the meeting at which the constitution was decided;
   b) Draft articles of association;

c) Declaration of commitment, signed by all the founders, that in the act of incorporation, and as a condition thereof, the assets required by law are fully paid up.

3. The declarations provided for in paragraph 1(c) may be submitted after the application has been submitted, under the terms and within the time limit laid down by the accrediting authority.

4. For the purposes of this law, significant holdings are those that equal or exceed 10% of the share capital of the public limited company.

5. The application for renewal of accreditation must be accompanied by the following documents:
   a) General program of activities planned for the next three years;
   b) A general description of the activities carried out in the last three years, and the balance sheet and accounts for the corresponding years, if any;
   c) Declaration that all the elements referred to in Article 72(1), (3) and (4) have not changed since they were submitted to the accrediting authority.

Article 22
Asset requirements

1. Private certifying bodies, which are legal persons, must have share capital of the minimum amount laid down in a joint decree issued by the members of the Government responsible for the areas of Finance and Communications, or, if they are not companies, equivalent assets.

2. The asset base, namely the company's minimum share capital, must always be fully paid up on the date of accreditation, if the legal person is already incorporated, or is always fully paid up with the incorporation of the legal person, if this occurs later.

Article 23
Suitability requirements

1. The members of the management and supervisory bodies, the employees, commissioners and representatives of the certifying entities with access to the certification acts and instruments, the partners of the company and, in the case of a public limited company, the shareholders with significant holdings must always be persons of recognized good repute.

2. Among other justifiable circumstances, it is considered indicative of a lack of good repute if the person has been:
   a) Convicted, at home or abroad, of theft, robbery, swindling, computer and communications fraud, extortion, abuse of trust, infidelity, forgery, false declarations, intentional insolvency, negligent insolvency, favoring creditors, issuing bad checks, abuse of guarantee or credit cards, illegitimate appropriation of public or cooperative sector assets, harmful administration in an economic unit of the public or cooperative sector, usury, bribery, corruption, unauthorized receipt of deposits or other repayable funds, unlawful practice of acts or operations inherent to the insurance or pension fund activity, money laundering, abuse of information, manipulation of the securities market or crime provided for in the Penal Code;

b) Declared bankrupt or insolvent by a national or foreign judgment or held liable for the bankruptcy or insolvency of a company it controls or of whose management or supervisory bodies it has been a member;
c) Subject to sanctions, at home or abroad, for breaches of the legal or regulatory rules governing the production, authentication, registration and conservation of documents, and in particular those of the notary's office, public records, the civil service, public libraries, and the certification of electronic signatures.

3. Failure to meet the suitability requirements set out in this article shall constitute grounds for refusal and revocation of accreditation, under the terms of Article 27(1)(c) and Article 27(1)(f).

Article 24
External security auditor

1. Accredited certification bodies must have an external safety auditor of recognized merit and reputation.

2. The auditor is responsible for regularly checking and evaluating the equipment and systems used in the certification activity, as well as issuing opinions, suggestions and recommendations, with a view to ensuring their efficiency, reliability and safety.
3. The auditor must submit an annual report to the accrediting authority by March 31st of each year, containing all the relevant data for monitoring the efficiency, reliability and safety of the equipment and systems used in the certification activity.

4. The appointment of the security auditor is subject to prior approval by the accrediting authority.

Article 25
Compulsory civil liability insurance

The characteristics of the civil liability insurance contract referred to in Article 20(1)(d) shall be defined by a joint ministerial decree issued by the members of the Government responsible for the areas of Finance and Communications.

Article 26
Decision

1. The accrediting authority may request additional information from applicants and carry out, by itself or by whoever it appoints for this purpose, the inquiries, investigations and inspections it deems necessary to assess the application.

2. The decision on the application for accreditation must be notified to the interested parties within 15 working days of receipt of the application or, where appropriate, of receipt of the additional information requested or the completion of any steps deemed necessary, but may not exceed six months from the date of receipt of the application.

3. The accrediting authority may include additional conditions in the accreditation provided that they are necessary to ensure compliance with the legal and regulatory provisions applicable to the exercise of the activity by the certifying entity.

4. The issuance of accreditation must be accompanied by the issuance by the accrediting authority of the certificate of keys to be used by the certification body in issuing certificates.

5. Accreditation shall be entered in the register referred to in Article 17(3) and published in Series II of the Official Gazette.

Article 27
Refusal of accreditation

1. Accreditation is refused whenever:
   a) The application for accreditation is not accompanied by all the necessary information and documents;
   b) The application form is inaccurate or untrue;
   c) The accrediting authority does not consider that any of the requirements listed in Articles 20 and 23 have been demonstrated.

2. If the application is inadequately instructed, the accrediting authority shall notify the applicant before refusing accreditation, giving them 30 days to remedy the deficiency.

Article 28
Accreditation expires

1. Accreditation expires in the following cases:
   a) When the certification activity is not started within 12 months of receiving the notification of accreditation;
   b) When, in the case of a legal person, it is dissolved, without prejudice to the acts necessary for its liquidation;
   c) When, after the expiration date, the accreditation has not been renewed.

2. The expiry of accreditation shall be entered in the register referred to in Article 17(3) and published in Series II of the Official Gazette.

Article 29
Revocation of accreditation

1. Accreditation is revoked, without prejudice to other sanctions applicable under the law, when any of the following situations occur:
   a) If it has been obtained through false declarations or other illicit means;
   b) If any of the requirements listed in Article 20 are no longer met;
   c) If the certification body ceases its certification activity or reduces it to an insignificant level for a period of more than 12 months;
   d) If there are serious irregularities in the administration, organization or internal supervision of the certification body;
   e) If, in carrying out the certification activity or any other social activity, unlawful acts are committed that damage or jeopardize public confidence in certification;
   f) If any of the circumstances of unfitness referred to in Article 48 supervenes in relation to any of the persons referred to in paragraph 1 thereof;
   g) If the certificates of the certification body referred to in Article 21(1)(f) have been revoked;
   h) Any modification made to the bylaws of certifying entities without the prior knowledge of the accrediting entity.

2. Revocation of accreditation is the responsibility of the accrediting authority, in a reasoned decision that must be notified to the organization within 8 working days.

3. The decision to revoke shall be entered in the register referred to in Article 17(3) and published in Series II of the Official Gazette.

Article 30
Anomalies in the management and supervisory bodies

1. If for any reason the legal and statutory requirements for the normal functioning of the administrative or supervisory bodies are no longer met, the accrediting authority sets a deadline for the situation to be rectified.

2. If the situation is not rectified within the time limit set, the accreditation will be revoked under the terms of the previous article.

Article 31
Computerized registration of certificates and conservation

1. Accredited certification bodies must organize and keep permanently updated a computer record of certificates issued, suspended, revoked or expired, which must be protected against unauthorized changes and be accessible to anyone for consultation, namely by computer means.

2. Certifying bodies must use reliable systems for keeping certificates in such a way that:
   a) Data entry and changes can only be made by authorized persons;
   b) Certificates may only be consulted by the public in cases where the holder's consent has been obtained;
   c) The authenticity of the information contained in the certificates can be verified;
   d) Any technical changes that could affect the system's security requirements can be detected immediately.

Article 32
Communicating changes

Changes to certifying bodies must be notified to the accrediting authority within 30 days:
   a) Company name;
   b) Object;
   c) Place of registered office, unless the change occurs within the same municipality or to a neighbouring municipality;
   d) Heritage substrate or heritage, as long as it is a significant change;
   e) Management and supervisory structure;
   f) Limiting the powers of management and supervisory bodies;
   g) Demerger, merger and dissolution;
   h) Any changes made to the bylaws.

Article 33
Registration of changes

1. The registration of the persons referred to in Article 21(1) must be requested from the accrediting authority within 15 days of their assuming any of the qualities referred to therein, at

the request of the certifying body or the interested parties, together with proof that they meet the requirements set out in that article, failing which the accreditation will be revoked.

2. The certifying body or the interested parties may request provisional registration before they assume any of the qualities referred to in Article 21(1), and conversion of the registration into definitive must be requested within 30 days of the designation, failing which it will lapse.

3. In the event of reappointment, this is entered in the register at the request of the certifying body or the interested parties.

4. Registration shall be refused in the event of unfitness, under the terms of article 23, and the refusal shall be communicated to the interested parties and to the certification body, which shall take the appropriate measures to ensure that they immediately cease to function or cease to be related to the legal person in the relationship provided for in the same article, following, where applicable, the provisions of article 31;

5. Without prejudice to other applicable legal provisions, failure to register does not in itself invalidate the legal acts carried out by the person concerned in the performance of their duties.

SUBSECTION II
CERTIFICATION ACTIVITY

Article 34
General role and duties of the certification body

1. The general task of the certification body is to ensure high levels of system security, which is essential for creating trust in electronic firms.

2. It is up to the certification body that issues certificates:
   a) Have the property requirements set out in Article 22;
   b) To offer guarantees of absolute integrity and independence in the exercise of the certification activity;
   c) Demonstrate the reliability required to carry out the certification activity;
   d) Maintain a valid insurance contract to adequately cover civil liability arising from the certification activity, under the terms of article 25;
   e) To have technical and human resources that meet safety and effectiveness standards, under the terms of the regulations;
   f) Use reliable systems and products that are protected against any modification and that guarantee the technical safety of the processes for which they are intended;
   g) Adopt appropriate measures to prevent the falsification or alteration of the data contained in the certificates and, in cases where the certification body generates signature creation data, guarantee its confidentiality during the creation process;

h) Use reliable systems for keeping certificates, so that:
   i. Certificates may only be consulted by the public in cases where the consent of their holder has been obtained;
   ii. Only authorized persons can enter data and changes to the certificates;
   iii. The authenticity of the information can be verified;
   iv. Any technical changes that could affect the safety requirements are immediately detectable.
i) Strictly verify the identity of the applicants holding the certificates and, in the case of representatives of legal persons, their powers of representation, as well as, where applicable, the specific qualities referred to in Article 42(1)(i);
j) Keeping evidence of the true identity of applicants holding pseudonymous certificates;
k) Inform applicants, in writing, in a complete and clear manner, about the process of issuing certificates and the exact terms and conditions of use of the certificate, including any restrictions on its use;
l) Comply with the security rules for processing personal data established in the respective legislation;
m) Do not store or copy signature creation data of the holder to whom the certification body has offered key management services;
n) Ensure the operation of a service that:
   i. Allows the computerized record of certificates issued, revoked, suspended or expired to be consulted quickly and securely;
   ii. Ensure the immediate and secure revocation, suspension or expiry of certificates;
o) Immediately publish the revocation or suspension of certificates, in the cases provided for in this statute;
p) Ensure that the date and time of issuance, suspension and revocation of certificates can be determined through chronological validation;
q) Offer and facilitate *time stamping* services (*digital time stamping - DST*) in the transmission and reception of data;
r) Keep the certificates it issues for a period of not less than 20 years.

3. The certifying entities, previously authorized by the accrediting authority, may delegate to the registration units the function of validating the identity and other data of the certificate subscribers, as well as the function of registering the presentations and procedures made to them.

Article 35
Chronological validation

1. Accredited certification bodies must be equipped with a chronological validation system for electronic documents, which can be used to provide services to the public.

2. The chronological validation system is approved by the accrediting authority, which must verify, in particular, the security, reliability and suitability of the date and time verification method.

3. The date and time contained in a chronological validation statement issued by an accredited entity are enforceable between the parties and against third parties.

Article 36
Data protection

1. Certifying entities may only collect personal data necessary for the exercise of their activities and obtain it directly from the persons interested in the ownership of key pairs and respective certificates, or from third parties from whom those persons authorize its collection.

2. Personal data collected by the certification body may not be used for any purpose other than certification, unless another use is expressly consented to by law or by the person concerned.

3. Certifying entities and the accrediting authority must comply with current legal regulations on the protection, processing and circulation of personal data and on the protection of privacy in the electronic communications sector.

4. Certifying bodies must communicate to the judicial authority, whenever the latter so orders under the legally stipulated terms, the data relating to the identity of the holders of certificates that are issued pseudonymously, following, where applicable, the regime established in criminal procedural legislation.

Article 37
Civil liability

1. The certification body is civilly liable for damages suffered by certificate holders and any third parties as a result of culpable failure to comply with the duties arising from this diploma and its regulations.

2. Exoneration and limitation of liability agreements provided for in the preceding paragraph shall be null and void.

3. Without prejudice to the provisions of the previous paragraph, certification bodies are not liable for damages resulting from the use of a certificate that exceeds the limits set for its use or the value of the transactions for which the certificate may be used, provided that these limits have been clearly brought to the attention of the holders through a declaration made on the certificate itself.

Article 38
Statement of certification practices

1. No accredited certification body may start issuing certificates without first ensuring adequate publicity for the certification practice statement, namely by computerized means.

2. The declaration of certification practices must comply with internationally recognized standards, without prejudice to its compliance with the provisions of this diploma.

3. The certification practice statement and any changes to it must be submitted to the accrediting authority for approval.

Article 39
Cessation of activity

1. If the certification body intends to voluntarily cease its activity, it must notify the accrediting authority and the persons to whom it has issued certificates that remain in force of this intention

at least three months in advance, also indicating the certification body to which it will forward its documentation or the revocation of the certificates at the end of that period, in which case it must place its documentation in the custody of the accrediting authority.

2. A certification body that is at risk of being declared bankrupt, undergoing company recovery proceedings or ceasing to operate for any reason beyond its control must immediately inform the accreditation authority.

3. In the case provided for in the previous paragraph, if the certifying entity ceases its activity, the accrediting authority shall promote the transfer of its documentation to another certifying entity or, if such transfer is impossible, the revocation of the certificates issued and the retention of the elements of such certificates for the period in which the certifying entity should have done so.

4. The cessation of the activity of a certification body that issues certificates shall be entered in the register referred to in Article 17(3) and published in Series II of the Official Gazette.

Article 40
Provision of certification services by third parties

1. Certification services can be provided and managed in whole or in part by third parties.

2. For the purposes of the previous paragraph, certification bodies must demonstrate their contractual relationship with the certification body that owns the technology.

3. The accrediting authority determines the conditions under which certification bodies can provide their services through a third party.

SECTION II
CERTIFICATES

Article 41
Issuing certificates

1. At the request of an interested natural or legal person and in their favor, the certification body issues the signature creation and verification data or, if requested, provides the technical means necessary for them to create them, and must always verify the identity and, where applicable, the powers of representation of the applicant by legally suitable and secure means.

2. At the request of the holder, the certification body issues one or more copies of the certificate and the complementary certificate.

3. The certification body must take appropriate measures to prevent the falsification or alteration of the data contained in the certificates and ensure compliance with the applicable legal and regulatory standards, using duly qualified personnel.

4. The certification body provides certificate holders with the necessary information for the correct and secure use of signatures, in particular information regarding:
   a) The obligations of the certificate holder and the certification body;
   b) The procedure for affixing and verifying signatures;
   c) The desirability of documents to which a signature has been affixed being re-signed when technical circumstances warrant it.

Article 42
Content of the certificates

1. The certificate must contain at least the following information:
   a) Name or denomination of the holder of the signature and other elements necessary for unequivocal identification and, where powers of representation exist, the name of his representative or authorized representatives, or a pseudonym of the holder, clearly identified as such;
   b) Name and electronic signature of the certifying entity, as well as an indication of the country in which it is established;
   c) Signature verification data corresponding to the signature creation data held by the owner;
   d) Serial number of the certificate;
   e) Start and end of validity of the certificate;
   f) Identifiers of algorithms used to verify the signatures of the holder and the certification body;
   g) Indication of whether or not the use of the certificate is restricted to certain types of use, as well as any limits on the value of the transactions for which the certificate is valid;
   h) Conventional limitations on the responsibility of the certification body, without prejudice to the provisions of Article 37(2);
   i) Any reference to a specific quality of the signature holder, depending on the use for which the certificate is intended;
   j) Indication that it is issued as a certificate.

2. At the request of the holder, information on powers of representation conferred on the holder by a third party, their professional qualifications or other attributes may be included on the certificate or on a supplementary certificate, provided that proof is supplied or that the information is unconfirmed.

Article 43
Suspension of certificate

1. The certification body suspends the certificate:
   a) At the request of the holder, duly identified for this purpose;
   b) When there is good reason to believe that the certificate has been issued on the basis of erroneous or false information, that the information it contains no longer conforms to reality or that the confidentiality of the signature creation data is not guaranteed.

2. Suspension on one of the grounds set out in point b) of the previous paragraph must always be justified and communicated to the holder within a maximum of 24 hours, as well as immediately

entered in the certificate register, and may be lifted when it is found that the grounds do not correspond to reality.

Article 44
Certificate revocation

1. The certification body revokes the certificate:
   a) At the request of the holder, duly identified for this purpose;
   b) When, after suspension of the certificate, it is confirmed that the certificate was issued on the basis of erroneous or false information, that the information contained therein no longer conforms to reality, or that the confidentiality of the signature creation data is not ensured;
   c) When the certification body ceases its activities without having transmitted its documentation to another certification body;
   d) When the accrediting authority orders the revocation of the certificate for legally justified reasons;
   e) When it becomes aware of the death, interdiction or disqualification of the natural person or the extinction of the legal person.

2. The decision to revoke the certificate on one of the grounds set out in points b), c) and d) of the preceding paragraph must always be substantiated and communicated to the holder, as well as immediately registered.

3. Revocation of the certificate has no retrospective effect.

Article 45
Common aspects of suspension and revocation

1. Suspension and revocation of the certificate shall be enforceable against third parties as soon as it is entered in the relevant register, unless it is proven that the third party was already aware of the reason for the suspension or revocation.

2. The certification body shall keep the information relating to the certificates for a period of not less than 20 years from the suspension or revocation of each certificate and shall make it available to any legitimate interested party.

3. The revocation or suspension of the certificate indicates the date and time from which it will take effect, and this date and time may not be earlier than the date on which this information is made public.

4. As of the suspension or revocation of a certificate, or the expiry of its validity period, the issuing of a certificate referring to the same signature creation data by the same or another certification body is prohibited.

Article 46
Obligations of the holder

1. The certificate holder must take all organizational and technical measures necessary to prevent damage to third parties and to preserve the confidentiality of all information transmitted.

2. Without prejudice to the precautions referred to in the preceding paragraph, the holder must also take reasonable measures when an electronic signature is supported by a certificate, in particular:
   a) Checking the validity, suspension or revocation of the certificate;
   b) The observance of any limitation relating to the certificate.

2. If there is any doubt as to the loss of confidentiality of the signature creation data, the holder must request the suspension of the certificate and, if the loss is confirmed, its revocation.

3. As of the suspension or revocation of a certificate or the expiry of its validity period, the holder is prohibited from using the respective signature creation data to generate an electronic signature.

4. Whenever there are reasons justifying the revocation or suspension of the certificate, the certificate holder must submit the corresponding request for suspension or revocation to the certification body within 24 hours.

5. The obligations laid down in this article shall apply, mutatis mutandis, to anyone who is listed on the certificate as represented.

Article 47
Certificates issued abroad

Without prejudice to the provisions of article 5, the accrediting authority shall disclose by the means of publicity it deems appropriate, as well as provide legitimate interested parties with the information it has on certificates issued by certification bodies based abroad that are recognized in Timor-Leste, or, at their request, on certification bodies accredited in foreign states.

CHAPTER IV
ACCREDITING AUTHORITY

Article 48
Appointment of accrediting authority

The functions of accreditation authority are assigned to the Information and Communication Technologies Agency I.P. (TIC TIMOR).

Article 49
Powers of the accrediting authority

The accrediting authority is responsible for:
   a) Accredit certifying bodies;
   b) Supervising certification bodies;
   c) Charging fees for accreditation services;
   d) Ensure that certifying bodies are liable for any damage caused to any entity or individual or legal entity that reasonably relies on the certificates;
   e) Auditing certification bodies;
   f) Ensure that security devices for creating electronic signatures comply with the conditions laid down in Article 34;

g) Entering into mutual recognition agreements with accreditation authorities in foreign countries, provided that this has been previously authorized by the member of the Government responsible;
h) Maintaining information on the internet about the list of certification bodies, and the suspension and revocation of digital certificates, as well as other relevant aspects of certification;
i) Define the technical requirements that qualify the suitability of the activities carried out by certification bodies;
j) Evaluate the activities carried out by authorized certifying entities, in accordance with the technical requirements defined under the terms of the previous paragraph;
k) Ensuring the proper functioning and efficient provision of services by certifying bodies, in accordance with the legal and regulatory provisions of the activity;
l) The rest that is entrusted to it by this statute and other complementary legislation.

Article 50
Other powers of the accrediting authority

The accreditation authority may require service providers that store information provided by the recipients of their services to act with the precautions that may reasonably be expected of them in order to detect and prevent illegal activities, as may be defined by law.

Article 51
Suspension and revocation of accreditation of certification bodies

1. The accreditation of the certifying entity is suspended whenever the certifying entity seriously fails to comply with the obligations laid down in this law.
2. The accrediting authority suspends accreditation for a maximum period of one month after hearing from the certification body.
3. In the event of a repeat offence or serious failure to comply with its obligations, the accreditation will be revoked.

CHAPTER VI
ELECTRONIC TRANSACTIONS

Article 52
Formation of electronic contracts

1. A contract may not be denied legal effect, validity or performance simply because an electronic communication, electronic record or electronic signature was used in its formation.

2 Unless otherwise agreed by the parties or specifically provided by other law, communications of tenders, acceptance of tenders and revocation of tenders and acceptances or any related communications may be expressed by electronic means.
3 Unless otherwise agreed by the parties, electronic contracts may be formed by means of an offer and acceptance of an offer expressed by electronic means, with reference to the following terms:
a) Time of sending, considering that an electronic communication is sent when the electronic communication first leaves an information system under the control of the sender or the party that sent it on behalf of the sender;

b) Time of receipt, whereby an electronic communication is deemed to have been received when it becomes accessible to the recipient at an electronic address designated by the recipient or, in any other case, when the recipient becomes aware that the electronic communication has been sent.
c) Place of sending, considering that an electronic communication is sent from:
   i. The workplace of the sending organization;
   ii. If the source entity has more than one place of business, the place of business that has the closest relationship to the underlying transaction; or
   iii. If there is no place of business to which point i) applies, the sender's main place of business;
   iv. In the case of a transferring entity that does not have a place of business, the usual place of residence of the sending entity;
d) Place of receipt, considering that an electronic communication is received:
   i. At the recipient's place of business;
   ii. If the recipient has more than one place of business, the place of business with the closest connection to the underlying transaction;
   iii. In the main establishment of the consignee, if there is more than one establishment and there is no establishment to which point (ii) applies;
   iv. In the case of a recipient who does not have a place of business, the recipient's usual place of residence;
   v. Time of communication of the acceptance of the offer, considering that, for the purposes of the formation of a contract, the acceptance of an offer by electronic communication is communicated to the tenderer at the time determined in point b) as the time of receipt of that electronic communication.

4. A contract may be formed through the interaction between an automated electronic system and an individual, acting on his own behalf or on behalf of another person, including an interaction in which, being free to refuse to perform, that same individual knows or has reason to know that by continuing he can cause the electronic agent to complete the transaction or performance.

5 In the event that a contract is formed through the interaction between an automated electronic system and a natural person, its validity cannot be denied simply because no natural person has analyzed or intervened in the actions performed by the automated system or in the resulting contract.

6. Where a natural person makes a mistake in entering data in an electronic communication exchanged with an automated electronic system of another party and that system does not give him the opportunity to correct the mistake, that person, or the person on whose behalf that person has acted, shall have the right to cancel the electronic communication in which the mistake was made.

7. The provisions of the preceding paragraph shall not apply unless the natural person, or the person on whose behalf that person has acted, is a natural person:
   a) notify the other party of the error as soon as possible after making or becoming aware of the error and indicate that it has made an error in the electronic communication;
   b) take reasonable steps, including steps in accordance with the reasonable instructions of the other person, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic registration;
   c) has not received or used any material benefit or value from the goods or services, if any, received from the other party.

(8) An offer to conclude a contract made by means of one or more electronic communications which is not addressed to one or more specific parties, but which is generally accessible to parties using information systems, including offers using interactive applications for placing orders through such information systems, shall be regarded as an invitation to tender, unless it clearly indicates the intention of the party making the offer to be bound in the event of acceptance.

Article 53
Obligations of e-commerce traders

1 The trader who engages in e-commerce or who uses e-commerce systems or services must provide all the information related to the use of e-commerce services, and this information must be displayed in a clearly visible manner on their e-commerce and e-sales website with the following details:
   a) Name of the e-commerce merchant;
   b) Tax Identification Number or, for traders who have their place of business outside Timor-Leste, the equivalent identification or taxpayer registration number issued by the competent authorities of the respective place of business;
   c) Geographical address where the e-commerce merchant is located;
   d) Contact details of the e-commerce trader, including at least a telephone number and email address.
   e) The price of any services or products offered on the respective marketing and sales website, including the currency in which the price is charged;
   f) Alternatives, if any, for the delivery of the product or service, the delivery rate for each of these alternatives and the estimated delivery rate for the product or service ordered;
   g) Method for reviewing and cancelling an order before it is definitively placed by the consumer;
   h) Terms and conditions applicable to the use of the e-commerce marketing and electronic sales site, which shall include, in particular:
      i. Information regarding the submission of consumer complaints or claims in relation to the e-commerce trader and the products or services offered by that trader, including the name, email address and telephone number of the person or service to which such complaints should be submitted;
      ii. Method and geographic location for resolving any disputes relating to any *online* purchase of services or products that cannot be resolved through the complaint process set out in the previous sub-paragraph, except where the location for dispute resolution is not in Timor-Leste, the terms and conditions specify an *online* dispute resolution mechanism, providing for mediation by a neutral third party to resolve the consumer's complaint.
      iii. Declaration that the e-commerce merchant complies with applicable data protection law and provides an *online* link to that law, if any;
      iv. Declaration that the e-commerce merchant complies with the provisions of article 56 of this Decree-Law regarding *Spam*.

2. In the event that mediation does not resolve the complaint or claim, the terms and conditions may specify that arbitration be used to resolve the dispute, which may take place *online,* in accordance with the rules established in the Timor-Leste Voluntary Arbitration Law.

3. The provisions of this article do not exclude the resolution of disputes based on machines, such as those provided by means of Artificial Intelligence, applicable under the terms regulated by Timorese law.

Article 54
Use of secure technologies and protocols

1. The e-commerce merchant must use secure technologies and protocols to safeguard the transmission and receipt of *online* payments and other private or sensitive information.

2. For any product or service ordered from the e-commerce merchant, the buyer must be provided with the following information before finalizing the purchase:
   a) The total price of the product or service, including any currency conversion fee, tax or delivery charge for the delivery method selected, in itemized form and listed separately;
   b) The payment methods accepted by the e-commerce merchant;
   c) The alternatives for returning, repairing or replacing a purchased product, as well as the deadlines applicable to each of them, in the event that the product delivered to the buyer is defective or does not correspond to the description of the product presented on the e-commerce trader's marketing and sales website;
   d) the time period and method by which a product delivered to the buyer may be returned to the seller, such period not being less than seven working days, and the apportionment of costs, if any, between the seller and the buyer for any returned product, unless the reason for the return is that the product is defective or does not conform to the description of the product provided by the e-commerce trader prior to its sale to the buyer, in which case the seller shall bear the full cost of returning the product.

3 An e-commerce merchant shall not produce or publish product or service reviews that it knows, or reasonably should know, are false or do not reflect the actual use of the product or service by consumers, and the provisions of articles 6 and 7 of the Timor-Leste Consumer Protection Law shall apply.

Article 55
Certification bodies

The conformity of electronic signature products with the technical requirements referred to in Article 21(1)(f) shall be verified and certified by the certification body at the Instituto Nacional de Qualidade, I. P..

Article 56
***Spam* ban**

1. It is prohibited for any sender of a commercial electronic mail message to send a message without including a return electronic mail address that is functional for at least 30 days after the transmission of the original message or provides another clearly displayed and readily accessible mechanism by which the recipient of the message can send, by electronic mail or other electronic communication, a request not to receive future messages from the sender at the specified electronic mail address.
2. The sending of commercial messages by e-mail is prohibited when the recipient has submitted a request not to receive such messages from a specific sender, made on a date corresponding to more than ten working days prior to the transmission of that unsolicited electronic message.

Article 57
Central supervisory body

1. A central supervisory body shall be set up to deal with e-commerce, except in matters where a special law assigns sectoral competence to another body.

2. The functions of the central supervisory body are exercised by TIC TIMOR.

3. The supervisory body shall act as a reference body for contacts in its field, providing information to recipients and the general public on request.

4. The supervisory body is responsible, in addition to the general duties already mentioned and those specifically assigned to it:
   a) Draw up regulations and give instructions on practices to be followed in order to comply with the provisions of this chapter;
   b) Monitoring compliance with e-commerce regulations;
   c) Initiating and investigating administrative offenses, as well as applying the sanctions provided for;
   d) To order the suspension of the activity of service providers in the face of serious irregularities and for reasons of urgency;
   e) Publicize the most significant codes of conduct of which you are aware on the web;
   f) Publicize other information, including court decisions in this area.

CHAPTER IV
DOWNLOADABLE ELECTRONIC RECORDS

Article 58
Application of complementary legislation

The provisions of this Decree-Law shall be without prejudice to the application to an electronic record of any rule of law governing a transferable document or instrument, including any rule of law applicable to consumer protection.

Article 59
Transferable documents or acts

1. Where the law requires a document or title to be transferable, this requirement shall be met by an electronic record, provided that:
   a) the electronic record contains information that must be included in a transferable document or instrument;
   b) a reliable method is used to:
      i. Identify that electronic record as the transferable electronic record
      ii. Make that electronic record subject to control from the moment it is created until the moment it ceases to have effect or is no longer valid;
      iii. Maintain the integrity of this electronic record.

2. The criterion for assessing integrity is whether the information contained in the downloadable electronic record, including any authorized change that occurs from its creation until its termination of effect or validity, remains complete and unaltered, with the exception of any change that occurs in the normal course of communication, storage and display.

3. The provisions of this Decree-Law shall be without prejudice to the inclusion of information in a transferable electronic record other than that contained in a transferable document or instrument.

Article 60
Control of electronic registration

1. Where the law requires or permits possession of a transferable document or instrument, that requirement shall be satisfied in relation to a transferable electronic record if a reliable method is used to:
   a) Establish exclusive control of that transferable electronic record by one person;
   b) Identify the person referred to in the previous paragraph as the person exercising control.

3. Where the law requires or permits the transfer of possession of a transferable document or instrument, that requirement or permission shall be fulfilled in relation to a transferable electronic record by the transfer of control over it.

Article 61
Indication of date and place on downloadable electronic records

Where the law requires or permits the indication of the time or place in relation to a transferable document or instrument, that requirement shall be satisfied if a reliable method is used to indicate that time or place in relation to a transferable electronic record.

Article 62
Endorsement

Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement shall be satisfied, in respect of a transferable electronic record, if the information necessary for the endorsement is included in the transferable electronic record and that information complies with the requirements set out in Article 59(2).

Article 63
Amendment

Where the law requires or permits the amendment of a transferable document or instrument, that requirement shall be satisfied in relation to a transferable electronic record if a reliable method is used for the amendment of the information contained in the transferable electronic record so that the amended information is identified as such.

Article 64
Replacement of a transferable document or instrument by a transferable electronic record

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

2 In order for the change of medium to take effect, a statement indicating the change must be entered in the electronic transfer register.

3 Once the electronic transferable record has been issued in accordance with paragraphs (1) and (2), the transferable document or instrument shall become unusable and shall cease to have any effect or validity.

4. The change of medium in accordance with paragraphs 1 and 2 shall be without prejudice to the rights and obligations of the parties.

Article 65
Replacing a transferable electronic record with a transferable document or instrument

1. A transferable document or instrument may replace a transferable electronic record if a reliable method of change of medium is used.

2. In order for the change of medium to take effect, a statement indicating this change must be inserted in the transferable document or instrument.

3. After the issuance of the transferable document or instrument in accordance with paragraphs (1) and (2), the transferable electronic record shall be rendered inoperative and shall cease to have any effect or validity.

4. The change of medium in accordance with paragraphs 1 and 2 shall be without prejudice to the rights and obligations of the parties.

Article 66
Private international law

The provisions of this Decree-Law shall not preclude the application to electronic transfer records of the rules of private international law governing a transferable document or instrument.

CHAPTER V
SANCTIONS AND MONITORING

SECTION I
PENALTY SYSTEM

Article 67
Sanctions

Without prejudice to other consequences provided for by law and to civil and criminal liability, any violation or non-compliance with the provisions of this law constitutes an administrative offense and is punishable by fines.

Article 68
Administrative offenses

These constitute administrative offenses:
a) Failure by certification bodies to comply with the obligations set out in Article 12;
b) Failure by e-commerce traders to comply with the obligations set out in articles 53 and 54;
c) Violation of Articles 34, 36 and 42;

d) Violation of Articles 24, 38, 39, 76(3) and (4) of the Civil Code;
e) Violation of other mandatory provisions in other cases by the certifying entities.

Article 69
Classification of offenses

1. The infractions referred to in points a) to d) of the previous article are considered serious.
2. Other situations of non-compliance referred to in point e) of the previous article are considered minor infringements.
3. Negligence is punishable within the limits of the fine applicable to the infringements provided for in the preceding paragraph.
4 Where the infringement is committed by a person other than a natural person, the fine shall be increased by one third, both as regards its maximum amount and its minimum amount.
5. The amount of the fine to be imposed on the offender, under the terms of this article, is set taking into account the seriousness of the infringement, which is determined by the following factors
   a) The extent of the damage caused;
   b) The amount of economic damage resulting from the infringement
   c) The frequency and duration of the behavior through which the infringement was committed
   d) The damage caused was reasonably foreseeable;
   e) Recidivism;
   f) The financial situation of the offender;
   g) Malice;
   h) The payment of some compensation to the injured party.

Article 70
Sanctions

1. Infringements committed under this law are punishable by the following penalties:
   a) A fine of between 500,000$ and 1,000,000$00 (five million escudos) for e-commerce traders violating the obligations set out in articles 53 and 54;
   b) A fine of US$ 100,000.00 to US$ 500,000.00 for violation of Articles 34, 36 and 42.
   c) A fine of US$ 50,000.00 to US$ 1,000,000.00 for violation of Articles 34, 36 and 42.
   d) A fine of US$ 50,000.00 to US$ 200,000.00 for violation of Articles 24, 38, 39, 76(3) and (4);
   e) Fines of between US$1,000.00 and US$2,000.00 in all other cases of non-compliance by certifying bodies.
2. Issuing certificates without having complied with the provisions of Article 17(2) shall be punishable under the terms of point a) of the previous paragraph.

Article 71
Accessory sanctions

1. The above-mentioned administrative offenses may be subject to the ancillary sanction of seizure of assets that are the vehicle for committing the infraction.

2. Depending on the seriousness of the infraction, the agent's guilt or the recidivism of the infractions, the accessory sanction of closure of the establishment or revocation of the certificate may be applied at the same time as the fines provided for in the previous article.

3.

Article 72
Advertising

Adequate publicity may be given to the punishment for an administrative offense, as well as to the ancillary sanctions applied under the terms of this law.

Article 73
Destination of fines

The amount of the fines collected is state revenue.

Article 74
Competence to investigate and decide on the administrative offense procedure

It is the responsibility of the accrediting authority to initiate and investigate the procedures relating to the infringements provided for in this statute, as well as the application of the respective penalties.

Article 75
Resource

1. The accrediting authority's decision may be appealed.
2. In appeals against decisions taken by the accrediting authority in the exercise of its accreditation, supervision and inspection powers, it is presumed, until proven otherwise, that the suspension of the effectiveness of the decision causes serious damage to the public interest.
3.

SECTION II
SURVEILLANCE

Article 76
Supervision of certification bodies

1. The accrediting authority may inspect the establishments used in the certification activity and examine documents, objects, equipment and operating procedures on site, and may make any necessary copies and records during the inspection.

2. Certifying entities must provide the accrediting authority promptly and exhaustively with all the information it requests for the purposes of supervising their activity.

3. Accredited certification bodies must notify the accrediting authority, within a maximum of 48 hours, of any changes to the elements referred to in articles 55 and 56, as well as all situations that determine or may determine the cessation of their activity.

4. By the last working day of each semester, accredited certification bodies must send the accrediting authority an updated version of the lists referred to in Article 46(1)(b).

Article 77
Duty to communicate

Persons or entities that provide auditing services to accredited certification bodies must report to the accrediting authority any infringements they detect in the course of their duties, as well as the

occurrence of situations that could jeopardize the efficiency, reliability and safety of the equipment and systems used in the certification activity.

Article 78
Cooperation from the authorities

The accrediting authority may ask the police and judicial authorities and any other public authorities and services for any collaboration or assistance it deems necessary for the accreditation and supervision of the certification activity.

Article 79
Application of special schemes

The regime established in this chapter is without prejudice to the application of the special regimes of administrative sanctions in force, provided for in other legislation.

Article 80
Subsidiary right

The sanctioning regime provided for in this statute is subsidiarily applicable, including as regards procedural rules, to the Regime of Administrative Offenses against the Economy and Food Safety, approved by Decree-Law no. 23/2009, of August 5, as amended by Decree-Law no. 43/2023, of May 31, which proceeds to its third amendment.

CHAPTER VI
FINAL PROVISIONS

Article 81
Regulations

This decree-law must be regulated in accordance with its provisions.

Article 82
Entry into force

This decree-law shall enter into force on the ninetieth day following its publication.

Approved by the Council of Ministers on ____ of _____ of _____

The Prime Minister

_____

Kay Rala Xanana Gusmão

The Minister of Finance

_____

Santina José Rodrigues Ferreira Viegas Cardoso

The Minister of Transport and Communications

_____

Miguel Marques Gonçalves Manetelu

The Minister for Trade and Industry

_____

Filipus Nino Pereira

Promulgated on ____ of _____ of _____

To be published.

The President of the Republic,

_____

José Ramos-Horta
