No. 37 of 2016.

Evidence (Amendment) Act 2016.

Certified : 13 DEC 2016

No. 37 of 2016.

Evidence (Amendment) Act **2016.**

ARRANGEMENT OF SECTIONS.

No. of 2016.

An Act

entitled

***Evidence (Amendment) Act* 2016,**

Being an Act to amend the ***Evidence Act*** (Chapter 48) to provide for admissibility of electronic evidence, and for related purposes,

MADE by the National Parliament to come into operation in accordance with a notice in the National Gazette by the Head of State, acting on advice.

1. INTERPRETATION (AMENDMENT OF SECTION 1).

Section 1 of the Principal Act is amended by deleting the words "and includes a part of a document" from the definition of "document" and replacing them with the following words:

"a part of a document, or an electronic form of such documents including documents produced using an electronic system or device".

2. REPEAL AND REPLACEMENT OF SECTION 8.

Section 8 of the Principal Act is repealed and replaced with the following new section:

"**8. IMAGES OF SEALS, SIGNATURES, ETC.**

(1) Where -

(*a*) a law requires a Court to take judicial notice of the seal or signature of a court or person appearing on a document; and

(*b*) a reproduction of the document is admitted in evidence under this Act in any legal proceedings,

the Court shall take judicial notice of the image of the seal or signature on the reproduction to the same extent as it would be required to take judicial notice of the seal or signature on the document.

(2) For the purposes of this section, seals and signatures include electronic seals, electronic signatures, and electronic certificates, or any other electronic form of verification.".

3. BUSINESS RECORDS (AMENDMENT OF SECTION 61).

Section 61 of the Principal Act is amended -

(*a*) by repealing Subsection (1) and replacing it with the following new subsection:

"(1) In this section -

"electronic form" in relation to records or data means data recorded or stored in a manner that requires an electronic system or device to display, interpret, and process it and includes documents (whether texts, graphics or spreadsheets) generated by a software and stored on disks or compact disks, DVDs, as well as electronic mail documents transmitted in electronic data interchange (EDI);

"record" means recorded data collected, created or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide evidence or proof of that activity or transaction, inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic system or device, or any other medium and is accessible in a perceivable form;

"writing" includes a photographic or photostatic reproduction, or electronic form of a document."; and

(*b*) in Subsection (4) -

(i) by deleting the full-stop at the end of Paragraph (*b*) and replacing it with "; and"; and

(ii) by adding, after Paragraph (*b*), the following new paragraph and full-stop:

"(*c*) where the writing is in electronic form, that it is -

(i) accessible so as to be usable for subsequent reference; and

(ii) capable of being retained by the recipient."; and

(*c*) by adding, after Subsection (5), the following new subsection:

"(6) For the purposes of determining the admissibility of a business record in electronic form, the provisions of Division 5 shall apply.".

4. REPEAL AND REPLACEMENT OF DIVISION IV.5.

Part IV of the Principal Act is amended by repealing Division 5 and replacing it with the following:

"***Division 5. - Electronic Evidence.***

64. INTEPRETATION OF DIVISION 5.

(1) In this Division, unless the contrary intention appears -

"accredited certificate" means a certificate issued by an accredited certification service;

"addressee" in relation to an electronic data, means a person

who is intended by the originator to receive such electronic data, and does not include a third party or an agent;

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

"communication" includes any communication of content -

(*a*) whether between persons, things, or persons and things; and

(*b*) in any combination or form, including speech, music or other sounds, data, text, writing, signs, signals or images (animated or otherwise);

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

"computer program" means data representing instructions or statements that, when executed in a computer or other electronic device, causes the computer or electronic device to perform a function;

"content" means data in any combination of form including speech, music or other sounds, text, writing, signs, signals or images (animated or otherwise);

"content data" means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form and includes any data that conveys the meaning or substance of a communication as well as data processed, stored, or transmitted by computer programs;

"cryptography service" means any service which is provided to a sender or recipient of an electronic communication, or to anyone storing an electronic communication, and is designed to facilitate the use of cryptographic techniques

for the purpose of ensuring -

(*a*) that the data or electronic communication can be accessed or put into an intelligible form only by certain persons; or

(*b*) that the authenticity or integrity of the data or electronic communication is capable of being ascertained; or

(*c*) the integrity of the data or electronic communication; or

(*d*) that the source of the data or electronic communication can be correctly ascertained;

"data" means any representation of facts, concepts, information (being either text, video, audio, or images), machine readable code or instructions, in a form suitable for processing in an electronic system including a program suitable to cause an electronic system to perform a function;

"device" includes but is not limited to -

(*a*) components of electronic systems such as a computer, graphic card, mobile phone, memory chip; or

(*b*) storage components such as a hard drive, memory card, compact disk, DVD, tape; or

(*c*) input devices such as a keyboard, mouse, track pad, scanner, digital camera; or

(*d*) output devices such as a printer, monitor, screen;

"electronic agent" means a program, electronic system or device, or other electronic or automated means configured and enabled by a person that is used to initiate or respond to an electronic record or event in whole or in part, without human intervention;

"electronic authentication" means any procedure used to verify that an electronic communication is that of the originator and that it has not been altered during transmission;

"electronic certificate" means a set of data or information enabling identification of the holder of the certificate, secure exchange of communication, data or information with other persons or institutions, and electronic form of data sent in such a way as to enable verification of its integrity and origin;

"electronic communication" means a transmission of data in any form by means of guided or unguided electromagnetic energy;

"electronic output" means a statement or a representation whether in written, printed, pictorial, film, graphical, audio or other form -

(*a*) produced by a computer or other electronic device; or

(*b*) displayed on the screen of a computer or other devices; or

(*c*) accurately translated from a statement or representation so produced;

"electronic record" means a set of data that is created, generated, recorded, stored, processed, sent, communicated or received, on any physical medium by an electronic system or device, and that can be read or perceived by a person by means of an electronic system or device, including a display, print out or other output of those data, such as, audio, video or audiovisual recordings, photographic images, and may or may not have a paper record to back it up;

"electronic signature" means any symbol or other data in electronic form or any methodology or procedure employed or adopted by a person with the intention of authenticating or verifying a record and includes an advanced electronic signature as provided by an accredited certification service provider, or a digital signature which is a particular type of electronic signature using digital technology;

"electronic system" means a system consisting of hardware or software, or a group of interconnected or related systems or devices, one or more of which, under a program, performs automatic (that is without direct human intervention) processing, generating, sending, receiving, or storing, of data and includes, but is not limited to, electronic devices, the internet input, output and storage facilities;

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

"location data" means any data processed in an electronic communications network indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

"originator"in relation to an electronic record, means a person who -

(*a*) sends an electronic record; or

(*b*) instructs another to send an electronic record on his behalf; or

(*c*) has an electronic record sent by his electronic agent but does not include any person acting as an agent or intermediary with respect to the sending of that electronic record;

"person" means an individual or body corporate;

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

"subscriber information" means any information contained in the form of electronic data or any other form that is held by a service provider, relating to the subscribers of its services, other than traffic data or content data, and by which can be established -

(*a*) the type of communications service used, the technical provisions take thereto, and the period of service; or

(*b*) the subscribers identity, postal or geographic address, telephone and other access number, billing and payment information, as it is available on the basis of the service agreement or arrangement; or

(*c*) any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement;

"traffic data" means any data relating to electronic communication by means of a computer program, computer, electronic system, or network, generated by a computer program, computer, electronic system, or network that forms a part, in the chain of electronic communication's origin, destination route, format, intent, time, date, size, duration, or type of underlying service and includes packet headers, pen register and trap and trace data.

(2) Where during a period the function of storing or processing data for the purposes of activities regularly carried on over the period, whether for profit or not, was regularly performed using an electronic system or device, all the electronic systems or devices used for that purpose during the period shall be treated, for the purposes of this Division, as constituting a single electronic system or device, and references in this Division to an electronic system or device shall be construed accordingly.

(3) For the purposes of this Division -

(*a*) a reference to data being derived from other data is a reference to its being derived from it by calculation, comparison or any other process; and

(*b*) data shall be taken to be supplied to an electronic system or device if it is supplied in any appropriate form and whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment; and

(*c*) where, in the course of activities carried on by a person, data is supplied with a view to its being stored or processed for the purposes of the activities by an electronic system or device operated otherwise than in the course of the activities, the data, if duly supplied to the electronic system or device, shall be taken to be supplied to it in the course of the activities; and

(*d*) an electronic record shall be taken to have been produced by an electronic system or device whether it was produced by it directly or (with or without human intervention) by means of any appropriate device.

(4) The provisions of this Division shall be interpreted and enforced in light of the internationally accepted principles of technological neutrality and of functional equivalence.

65. ADMISSIBILITY OF ELECTRONIC EVIDENCE.

(1) In applying any existing rules or statutory provisions relating to the admissibility of records, the Court may have regard to the principles guiding the admissibility of electronic records as prescribed under this Division.

(2) Nothing in this Act or any rules governing evidence shall apply to deny the admissibility of electronic evidence solely on the ground that it is in electronic form.

66. EXISTING RULES OF EVIDENCE.

The provisions of this Division are in addition to and not in derogation of any powers, rights or rules of evidence given or prescribed by this Act or any other law.

67. INTEGRITY OF ELECTRONIC SYSTEMS.

(1) Subject to Subsection (2), in any legal proceedings, where the original of an electronic record is required to be given in evidence, the requirement is satisfied on proof of the integrity of the electronic system or device by which the data was recorded or stored.

(2) In the absence of evidence to the contrary, the integrity of the electronic system or device in which the electronic record is recorded or stored is presumed in any legal proceeding where -

(*a*) evidence is given that supports a finding that -

(i) at all material times the electronic system or device was operating properly; or

(ii) if at any time the electronic system or device was not operating properly or was out of operation, the integrity of the record was not affected by such circumstances; or

(iii) there are otherwise no other reasonable grounds to doubt the integrity of the record; or

(*b*) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(*c*) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

67A. PROOF OF ELECTRONIC RECORDS.

(1) In any legal proceedings, a statement contained in an electronic record produced by an electronic system or device shall not be admissible as evidence of any fact stated in the electronic record of which direct oral evidence would be admissible, unless the integrity of the electronic system or device is presumed under Subsection (2).

(2) In the absence of evidence to the contrary, the integrity of the computer in which an electronic record is recorded or stored is presumed in any legal proceedings if the transaction record -

(*a*) has remained complete and unaltered, apart from -

(i) the addition of any endorsement; or

(ii) any immaterial change,

which arises in the normal course of communication, storage or display; or

(*b*) has been electronically certified or has been electronically signed, by a method provided by accredited certification entities; or

(*c*) which integrity and content has been notarised; or

(*d*) has been recorded in a non-rewritable storage device, or any other electronic means that does not allow the alteration of the electronic records; or

(*e*) has been examined and its integrity confirmed by an expert appointed by the Court; or

(*f*) relating to which -

(i) evidence is adduced that supports a finding that, at all material times, the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record; or

(ii) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(iii) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(3) For the purpose of deciding whether or not a statement in an electronic record is admissible in evidence under this section, the Court may draw any reasonable inference from the circumstances in which the statement was made or otherwise came into being or from any other circumstances (including, in the case of a statement contained in an electronic record, the form and contents of that electronic record).

(4) Where, in any legal proceedings, it is desired to give a statement in evidence under this Division, a certificate -

(*a*) identifying the electronic record containing the statement and describing the manner in which it was produced; or

(*b*) giving such particulars of any electronic system or device involved in the production of the electronic record as are appropriate for the purpose of showing that the electronic record was produced by an electronic system or device; or

(*c*) dealing with any of the matters referred to in Section 64(3), and signed by a person -

(i) occupying a responsible position in connection with the management of the relevant activities; or

(ii) having technical expertise in relation to the operation of the relevant electronic system or device,

is evidence of any matter stated in the certificate.

67B. PRINTOUTS.

Where, in any legal proceedings, a statement contained in an electronic record is proposed to be given in evidence under this Division, it may be proved by the production of the electronic record or (whether or not

the electronic record is still in existence) by the production of a printout of the electronic record or of the material part of the electronic record, if the electronic record in the form of a printout has been -

(*a*) manifestly or consistently acted on; or

(*b*) relied upon; or

(*c*) used,

as the record of the data recorded or stored on the printout.

67C. BURDEN TO PROVE AUTHENTICITY.

In any legal proceedings, the burden of proving the authenticity of electronic records lies with the party proposing to give it in evidence.

67D. STANDARDS.

(1) For the purposes of this section, 'Authority' means the body responsible for regulating the Information and Communication Technology industry including the development or approval of relevant technical standards or cybersecurity procedures.

(2) For the purpose of determining, under this Act or any other law, whether an electronic record is admissible -

(*a*) evidence may be given in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour used, recorded or preserved, the electronic record and the nature and purpose of the electronic record; and

(*b*) the Authority may issue guidelines providing orientation on the applicable criteria to be followed for purposes of this Division.

67E. AFFIDAVITS.

Where a party to or a person interested in any legal proceeding desires to give an electronic record in evidence, he may do so in the form of an affidavit.

67F. CONSENTING TO ADMISSIBILITY OF EVIDENCE.

(1) Subject to Subsection (2), and unless otherwise provided in this Act or any other law, an electronic record is admissible, subject to the discretion of the Court, if the parties to the proceedings have expressly consented at any time that its admissibility may not be disputed.

(2) A consent entered into under Subsection (1) does not render the record admissible in a criminal proceeding if, at the time the consent was reached, the accused person or any of the persons accused in the proceeding was not legally assisted or represented.

67G. ELECTRONIC SIGNATURE.

(1) An electronic signature is not without legal force and effect merely on the ground that it is in electronic form.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

(3) Where the law requires the signature of a person, the requirement is met by an electronic signature if the electronic signature that is used is as reliable and as appropriate for the purpose for which it was generated or communicated, in all the circumstances including any relevant agreements.

(4) Subsection (3) applies whether the requirement for signature is in the form of an obligation or the law provides consequences for the absence of a signature.

(5) Parties may agree to use a particular method of electronic signature, unless otherwise provided by law.

(6) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, the requirement is met in relation to the data message if -

(*a*) the signature creation data is linked to the signatory and no other person; and

(*b*) the signature creation data at the time of signing is under the control of the signatory and no other person; and

(*c*) any alteration to the electronic signature, made after the time of signing is detectable; and

(*d*) where a purpose of the legal requirement for a signature is to provide assurance as to the soundness of the data to which it relates, any alteration made to the data after the time of signing is detectable.

(7) Subsection (6) does not limit the ability of a person to -

(*a*) establish in any other way, for the purpose of satisfying the requirement under Subsection (3), the reliability of an electronic signature; or

(*b*) adduce evidence of the non-reliability of an electronic signature.

(8) A person relying on an electronic signature shall bear the legal consequences of his failure to take reasonable steps to verify the reliability of an electronic signature.

67H. ALTERNATIVE TECHNIQUES AND PROCEDURES FOR PRODUCTION OF ELECTRONIC EVIDENCE.

In addition to the means of proof referred to in the preceding sections in this Division, electronic evidence may be produced with regard to certain electronic records by means of alternative techniques and procedures, such as attestation by notaries public or justices of the peace or by other such authorities, recording on non-rewritable medium, and electronic forensics in the course of judicial discovery.

67I. ADMISSIBILITY OF ELECTRONIC RECORDS FROM OTHER COUNTRIES.

(1) Where electronic evidence originates from another jurisdiction, its admissibility is not impaired if the integrity of the electronic system or device associated with the relevant electronic evidence is proven or presumed in accordance with Section 67(2)(*a*) and Section 67A(2) of this Act.

(2) In determining whether or not, or to what extent, record in electronic form is legally effective, it is immaterial where the record was created or used or the place of business of its creation, provided the electronic record is located in domestic jurisdiction.

(3) Where the electronic record is located in a foreign jurisdiction, it will not be admissible unless -

(*a*) notice of a party's desire to give such evidence, accompanied by an affidavit containing a copy of the contents of the electronic record proposed to be given in evidence, is served on each other party not less than 14 clear days before the hearing; or

(*b*) the Court directs that it is to apply; or

(*c*) there is an international treaty in effect establishing recognition of electronic records or of electronic signature located in the foreign jurisdiction.

67J. WEIGHT TO BE ATTACHED TO ELECTRONIC RECORDS.

In estimating the weight (if any) to be attached to a statement in an electronic record admissible in evidence under this Division, regard shall be had -

(*a*) to all the circumstances from which an inference can reasonably be drawn as to the accuracy or otherwise of the statement or the electronic record; and

(*b*) to the question, whether or not the data contained in the statement or electronic record is reproduced or derived from -
  (i) was supplied to the electronic system or device; or
  (ii) was recorded for the purpose of being supplied to it, at the same time with the occurrence or existence of the facts dealt with in the statement or electronic record; and

(*c*) to the question, whether or not any person concerned with -
  (i) the supply of data to the electronic system or device; or
  (ii) the operation of the electronic system or device by means of which the electronic record containing the statement was produced,

had any incentive to conceal or misrepresent the facts.".

I hereby certify that the above is a fair print of the ***Evidence (Amendment) Act*** **2016** which has been made by the National Parliament.

Acting Clerk of the National Parliament.

13 DEC 2016

I hereby certify that the ***Evidence (Amendment) Act*** **2016** was made by the National Parliament on 11 August 2016.

Acting Speaker of the National Parliament.

13 DEC 2016