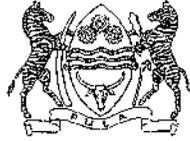


ELECTRONIC RECORDS (EVIDENCE) ACT, 2014

No. 13



of 2014

ARRANGEMENT OF SECTIONS

SECTION

1. Short title and commencement
2. Interpretation
3. Application
4. Derogation from rule of law on authentication and best evidence
5. Admission and authentication of electronic records
6. Evidence of electronic records
7. Application of best evidence rule to electronic records
8. Admissibility of electronic signature
9. Presumption of integrity
10. Standards, etc. may be considered
11. Proof by affidavit
12. Powers of court to call for further evidence
13. Assessing evidential weight of electronic record
14. Proof of matters
15. Offences and penalties
16. Regulations

An Act to provide for the admissibility of electronic records as evidence in legal proceedings and authentication of electronic records; to provide for the admissibility in evidence of electronic records as original records and for matters incidental and connected thereto.

Date of Assent: 14.05.14

Date of commencement: ON NOTICE

ENACTED by the Parliament of Botswana.

1. This Act may be cited as the Electronic Records (Evidence) Act, 2014 and shall come into operation on such date as the Minister may, by Order published in the *Gazette*, appoint.

Short title and commencement

2. In this Act, unless the context otherwise requires —

Interpretation

“Communications Regulatory Authority” means the Communications Regulatory Authority established under section 3 of the Communications Regulatory Authority Act;

Act No. 19 of 2012

“computer system” means an electronic, magnetic or optical device, or a group of interconnected or related devices, including the internet, one or more of which pursuant to a computer programme, performs automatic processing of data or any other function;

“court” includes a tribunal, board and commission;

“data” means —

- (a) any representation of facts, information or concepts in a form suitable for processing in a computer system;
- (b) an information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; or
- (c) a programme suitable to cause a computer system to function;

“electronic record” means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device, and includes a display, printout or other output of that data;

“electronic records system” includes a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic records;

“electronic signature” means data in electronic form attached to or logically subjoined to an electronic communication, and which can be used to identify the signatory (method of authentication) and indicate consent for the information contained in the said communication;

“evidence” includes all electronic records produced for the inspection of a court; and

“legal proceeding” includes administrative proceedings.

Application

3. This Act shall apply to any legal proceedings in or before any court and to affidavits presented to any court or officer of any court.

Derogation from rule of law on authentication and best evidence

4. This Act does not derogate from any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence, which rules are derogated from in the manner provided for in sections 6 and 7, respectively.

Admission and authentication of electronic records

5. (1) Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

(2) A court may have regard to evidence adduced under this Act in applying any common law rule relating to the admissibility of electronic records.

Cap. 08:02

(3) Notwithstanding section 244 of the Criminal Procedure and Evidence Act, in so far as it relates to the signing and certification of a copy of, or extract from a book or record as true copy or extract, and subject to subsection (4), a person may seek the admission of such copies or extracts from a book or record and of entries in bankers’ books in electronic form as evidence in any legal proceedings.

(4) A person who seeks to admit an electronic record in any legal proceedings as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is that which he or she purports it to be.

(5) Notwithstanding section 245 of the Criminal Procedure and Evidence Act, any Government officer who has the custody or control of a record by virtue of his or her office shall produce that record in an electronic form in any criminal or civil proceedings before any court on a preparatory examination upon the order of the Director of Public Prosecutions.

(6) It shall be sufficient to produce an extract from a banker's book, in electronic form, and such extract shall be admissible in evidence before any court, as the original record.

(7) Notwithstanding subsection (3), in so far as it relates to entries in bankers' books, and subsection (4), a person seeking to admit an electronic record as evidence of an entry in a banker's book shall comply with the proviso to section 248 (1) of the Criminal Procedure and Evidence Act.

6. (1) In this section "approved process" means a process that has been approved by a certifying authority in accordance with the provisions of any regulations made by the Minister.

Evidence of
electronic
records

(2) The Communications Regulatory Authority shall be the certifying authority for purposes of this Act.

(3) Unless otherwise provided in any other written law, where an electronic record is tendered in evidence, such an electronic record shall be admissible if it is relevant and is produced in an approved process.

(4) A certificate signed by the certifying authority purporting to identify the electronic records system including that part of the system that is relevant to the proceedings, shall be sufficient evidence of the integrity of the electronic records system.

(5) Where an electronic record is obtained from an electronic records system and duly certified as such by the certifying authority in relation to the operation or management of the approved process, it shall be presumed that it accurately reproduces the contents of the original record unless the contrary is proved.

(6) A certificate signed by a person holding a responsible position in relation to the operation or management of the relevant electronic records system in accordance with subsection (3) —

- (a) purporting to identify the electronic records system and describing the manner in which the electronic record was produced;
- (b) giving particulars of any device involved in the processing and storage of the electronic record; and
- (c) dealing with the matters mentioned in that subsection, shall be sufficient evidence of the matters stated in the certificate.

(7) If the person who holds a responsible position in relation to the operation or management of the electronic records system in accordance with subsection (6) did not have control or access over any relevant records and facts in relation to the production by the electronic records system of the electronic record, a supplementary certificate signed by another person who had such control or access and made in accordance with subsection (6), shall be sufficient evidence of the matters stated in the certificate.

(8) If a person referred to in subsection (6) or (7) refuses or is unable for any reason to certify any electronic record or electronic records system, a certificate signed by another person who had obtained or been given control or access to the relevant records and facts in relation to the production by the computer of the electronic record and made in accordance with subsection (6), shall be sufficient evidence of the matters stated in the certificate.

(9) For the purposes of subsections (4) to (8), it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(10) Any electronic record tendered in evidence under this section and duly authenticated shall be admissible as evidence of proof of the contents of the original record notwithstanding that —

- (a) certain parts or features of the original record, such as boxes, lines, shades, colours, patterns or graphics, do not appear in the record if such parts or features do not affect the accuracy of the relevant contents; or
- (b) it is secondary evidence.

Application of
best evidence
rule to
electronic
records

7. (1) The best evidence rule in respect of an electronic record shall be satisfied —

- (a) on proof of the integrity of the electronic records system in or by which the data contained in the electronic record was recorded or stored; or
- (b) if the electronic record contains an electronic signature that was added when the electronic record was first generated in its final form and that can be used to verify that the electronic record has not been changed since that time.

(2) Notwithstanding subsection (1), in the absence of evidence to the contrary, an electronic record in the form of a printout shall satisfy the best evidence rule if, in any legal proceedings, the printout has been consistently acted on, relied on or used as a record of the information recorded or stored in the printout.

Admissibility
of electronic
signature

8. (1) Where a rule of law requires a signature, or provides for certain consequences if the record is not signed, an electronic signature shall satisfy that requirement or shall operate to avoid those consequences.

(2) Subject to the Electronic Communications and Transactions Act, an electronic signature may be proved in any manner, including by showing that a method 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.

Act No. 14 of
2014

(3) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement, in relation to data, is met if an electronic signature is used.

9. For the purpose of section 5 (1) and 7 (1) (a), in the absence of evidence to the contrary, the integrity of an electronic records system by or which an electronic record is recorded or stored is proven –

Prestumption of
integrity

- (a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic records system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds to doubt the integrity of the electronic records system;
- (b) by the party tendering such record that there is no reasonable ground for believing that the electronic record is inaccurate because of improper use of the electronic records system and that no reason exists to doubt or suspect the truth or reliability of the electronic record;
- (c) if it is established that the electronic record was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
- (d) if 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 and who did not record or store it under the control of the party seeking to introduce it.

10. For the purpose of determining under any rule of law, whether or not an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the matter in which the electronic records are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

Standards, etc.
may be
considered

11. The matters referred to in sections 7 (2), 9 and 10 may be established by affidavit.

Proof by
affidavit

Powers of court to call for further evidence

12. (1) Where a court is not satisfied that the electronic record sought to be admitted in evidence under section 4 accurately reproduces the relevant contents of the original record, the court may, in its discretion, call for further evidence.

(2) Where further evidence is called for under subsection (1), such evidence may be established by an affidavit made by —

(a) a person holding a responsible position in relation to the operation or management of the certifying authority appointed under section 6 (2);

(b) any other person holding a responsible position in relation to the operation of the electronic records system at the relevant time;

(c) the person who had control or access over any relevant records and facts in relation to the production of the electronic record;

(d) the person who had obtained or been given control or access over any relevant records and facts in relation to the production of the electronic record; or

(e) an expert appointed or accepted by the court.

(3) Notwithstanding subsections (1) and (2), the court may, if it thinks fit, require that oral evidence be given of any matters concerning the authenticity of the electronic record, and may call a deponent of an affidavit under subsection (2) or any person responsible for a certificate issued under section 6 for this purpose.

Assessing evidential weight of electronic record

13. In assessing the evidential weight of any electronic record admitted under section 5, the court shall have regard to all the circumstances from which any inference can reasonably be drawn as to the authenticity or otherwise of the electronic record and, in particular —

(a) whether or not the information which the electronic record reproduced or is derived from was supplied to the relevant electronic records system, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information, if such contemporaneity is relevant; and

(b) whether the supplier of the information or any person involved in the processing of such information had any incentive or motive to conceal or misrepresent the information so supplied.

Proof of matters

14. (1) Without prejudice to sections 12 and 13, whenever the authenticity of any electronic record is proved under section 5, all matters may be proved in order to —

(a) contradict or corroborate it; or

(b) impeach or support the credibility of the person by whom it was made, or by whom the information was processed.

(2) Evidence may not be given under subsection (1) of any matter of which, if the person had been called as a witness and had denied that matter upon cross-examination, evidence could not have been adduced by the cross-examining party.

15. Any person who, in a certificate tendered under section 6, in a court makes a statement which he or she knows to be false or does not reasonably believe to be true commits an offence and is liable to a fine not exceeding P10 000, or to imprisonment for a term not exceeding five years, or to both.

Offences and
Penalties

16. (1) The Minister may make regulations providing for any matter which under this Act is to be provided for by regulations or for the better carrying out of the purposes and provisions of this Act.

Regulations

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations relating to —

- (a) the approved process for production of electronic records as evidence;
- (b) requirements for certificates; and
- (c) any other matter which requires to be prescribed under the Act.

PASSED by the National Assembly this 9th day of April, 2014.

BARBARA N. DITHAPO,
Clerk of the National Assembly.