ANGUILLA

A BILL FOR

ELECTRONIC EVIDENCE ACT, 2022

Published by Authority

ELECTRONIC EVIDENCE ACT, 2022

TABLE OF CONTENTS

I Assent

_____
Dileeni Daniel-Selvaratnam
Governor

_____
Date

ANGUILLA

No. /2022

A BILL FOR

ELECTRONIC EVIDENCE ACT, 2022

[Gazette Dated: , 2022] [Commencement: Section 19]

An Act to make provision for the legal recognition of electronic records and to facilitate the admission of such records into legal proceedings and other related matters.

ENACTED by the Legislature of Anguilla

PART 1

PRELIMINARY

Interpretation

1. In this Act—

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

"accredited certification entity" means an entity approved by the Government of Anguilla as an appropriate authority to determine accreditation certification under the provisions of this Act;

"addressee", in relation to an electronic record means a person who is intended by the originator of such electronic record to receive it, and does not include a person acting as an intermediary with respect to that electronic record;

"advanced electronic signature" means an electronic signature provided by an accredited certification service provider;

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

"certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person, or links time-verification data to an electronic record or to an electronic communication and confirm its date and time;

"computer" means any digital information system integrated by equipment and programs intended for creation, recording, storage, processing and/or transmission of data, including any computer, computer devices, or other electronic information or communication devices, intended to perform such functions;

"data (or computer data, or electronic data)" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

"digital signature" means an electronic signature based on asymmetric cryptography including associated public and private keys;

"electronic" includes created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic, optical or by any other means that has capabilities for creation, recording, transmission or storage similar to those means;

"electronic agent" means a program, computer, 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 review by an individual;

"electronic communication" means any transfer of records by means of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include—

(a) any oral communication;

(b) any communication made through a tone-only paging device;

(c) any communication from a tracking device;

"electronic record" means a set of data that is created, generated, recorded, stored, processed, sent, communicated, and/or received, on any physical medium by a computer or other similar device, that can be read or perceived by a person by means of a computer system or other similar device, including a display, print-out or other output of those data;

"electronic signature" means data in electronic form, incorporated into or otherwise logically associated with any electronic data or communications, and adopted by a person with the intent to indicate their approval and agreement to the content;

"information system (or computer system, or data processing system)" means a device or a group of inter-connected or related devices, including the internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

"law" means the common law, primary legislation, and subsidiary legislation;

"legal proceedings" means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission;

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

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

(a) sends an electronic record;

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

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

"public body" includes—

(a) ministry or department of government;

(b) wholly or partially owned state companies or enterprises;

(c) bodies exercising statutory authority, of a legislative, executive or judicial nature;

(d) sub-national or local public authorities;

"record" means recorded information 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 or any other medium and is accessible in a perceivable form;

"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 presumed to be that of a particular person or for detecting changes or errors in content of an electronic communication;

"signature" includes any symbol executed or adopted, or any methodology or procedure employed or adopted by a person with the intention of authenticating a record, including electronic or digital methods;

"signature creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

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

(a) the type of communication service used, the technical provisions taken thereto, and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other information that is capable of identifying the subscriber billing and payment information, as it is available on the basis of the service agreement or arrangement; and

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

"traffic data" means computer data that—

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of the chain of communication; and

(c) shows the communication's origin, destination, route, time, date, size, duration or type of underlying services.

PART 2

ADMISSIBILITY

Amendment to authentication and best evidence rules

2. This Act does not modify any common law or statutory provision relating to the admissibility of records, except those relating to authentication and best evidence.

Common law and statutory rules

3. In applying any common law or statutory provision relating to the admissibility of records, the Court may have regard to the principles guiding the admissibility of electronic records as prescribed by this Act.

General admissibility of electronic evidence

4. 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.

Application of the best evidence rule

5. (1) In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the computer in or by which the data was recorded or stored.

(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 proceeding—

(a) where 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 was 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;

(b) where it is established that the electronic record was recorded or stored by a party to the proceedings who has interests that are adverse to the party seeking to introduce it; or

(c) where 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.

Integrity of information and specific admissibility rules

6. (1) A statement contained in an electronic record produced by a computer which constitutes hearsay shall not be admissible in any proceedings as evidence of any fact stated therein unless the integrity of the computer 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 proceeding 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;

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

(c) integrity and content has been notarized;

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

(e) has been examined and its integrity confirmed by an expert appointed by a 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,

(ii) it is established that the electronic record was recorded or stored by a party to the proceedings who has interests that are adverse 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) Where a statement contained in an electronic record produced by a computer does not constitute hearsay, such a statement shall be admissible if the conditions specified in subsection (2) are satisfied in relation to that record.

Print-outs

7. In any legal proceeding, where an electronic recording in the form of a print-out has been manifestly or consistently acted on, relied on, or used as the record of the information recorded or stored on the print-out, the print-out is the record for the purpose of the best evidence rule.

Burden to prove the authenticity of electronic evidence

8. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Standards

9. For the purpose of determining under any other law whether an electronic record is admissible, evidence may be presented 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 that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

Affidavits

10. Where it is intended to adduce an electronic record as evidence, it is permissible to have that record adduced in the form of an affidavit.

Agreement on admissibility of evidence

11. (1) Unless otherwise provided in any statute, an electronic record is admissible, subject to the discretion of the Court, if the parties to the proceedings have expressly agreed at any time that its admissibility is not in dispute or may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not legally assisted or represented.

Electronic signature

12. (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.

Electronic signature requirements

13. (1) 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.

(2) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the law provides consequences for the absence of a signature.

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

(4) 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;

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

(c) an 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 information to which it relates, any alteration made to that information after the time of signing is detectable.

(5) Subsection (4) does not limit the ability of a person—

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of an electronic signature; or

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

(6) The Court shall have regard to any law that provides for the veracity of its authorship and integrity of digitally signed electronic records.

Alternative techniques and procedures for production of electronic evidence

14. In addition to the means of proof referred to in the preceding sections in this Act, electronic evidence may be produced with regard to certain electronic record 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 computer forensics in the course of judicial discovery.

PART 3

GENERAL PROVISIONS

Admissibility of electronic records from other countries

15. Where an electronic evidence originates from another jurisdiction, its admissibility is not impaired if the integrity of the computer associated with the relevant electronic evidence is proven or presumed in accordance with standards comparable to those provided for in section 5(2)(a), and 6(2) of this Act.

Recognition of foreign electronic documents and signatures

16. (1) In determining whether or not, or to what extent, information in electronic form is legally effective, no regard shall be had to the location where the information was created or used to be the place of business of its creation, provided the electronic record is located in a domestic jurisdiction.

(2) Where the electronic record is located in a foreign jurisdiction, subsection (1) above does not apply unless—

(a) the party who adduces evidence of the contents of the electronic record has, not less than 30 days before the day on which the evidence is adduced, served on each other party a copy of the electronic record proposed to be tendered;

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

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

Interpretation in accordance with internationally accepted principles

17. The provisions of this Act shall be interpreted and enforced in light of the internationally accepted principles of technological neutrality and of functional equivalence.

Regulations

18. The Governor, on the advice of the Attorney-General, may make regulations for giving effect to the purposes of this Act and for prescribing anything required or authorised by this Act to be prescribed, taking into consideration international best practices and standards.

Citation and commencement

19. This Act may be cited as the Electronic Evidence Act, 2022 and shall come into force on a day to be appointed by the Governor by Notice in the *Gazette*.

Barbara Webster-Bourne
Speaker

Passed by the House of Assembly this day of , 2022.

Lenox J. Proctor
Clerk of the House of Assembly