

Electronic Communications and Transactions Act 25 of 2002 (ECTA)

Topic: Information Technology and Electronic Communications

IN A CALABASH

Introduction

In order to legitimise electronic communications (fax, sms, email and voice messages), the government has introduced the Electronic Communications and Transactions Act (ECTA), which commercially recognises and gives legal force and effect to such electronic communications.

Objectives of the Act

The objective of ECTA is to provide for the facilitation and regulation of electronic communications and transactions and to prevent the abuse of information systems.

Application of the Act and its implication to Tourism

The ECTA applies to all persons and entities that make use of (i.e. send and receive) electronic communications and data messages.

Summary of the provisions of the Act

Legal requirements for data messages

The ECTA gives legal recognition to any data message. A 'data message' is defined under the ECTA to mean and include data generated, sent, received or stored by electronic means, including voice where the voice is used in an automated transaction and stored records.

Requirement for writing

The ECTA states that when there is a requirement that a document or information must be in writing, this will be met if the document or information is in the form of a data message and is accessible so as to be usable for later reference.

Requirement for signature

The ECTA allows any contract or document to be signed electronically. The reader should also take note that an electronic signature is not without legal force and effect merely because it is in electronic format. The ECTA makes reference to two types of signatures – an advanced electronic signature and an electronic signature.

‘Advanced electronic signature’ means a security protected and enabled electronic signature which is encrypted and can only be used by the owner. This ‘encrypted product’ has to be accredited under the ECTA.

‘Electronic signature’ means data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature.

The ECTA states that when any document has to be signed in terms of a specific law, the person who is required to sign the document or contract may only sign such document using an advanced electronic signature. In this regard, take note that an advanced electronic signature is regarded as valid and properly applied unless the contrary is proved.

In the absence of a specific law requiring signature, when one party requires another party to sign a document, an electronic document may be signed by applying an electronic signature to the document. Following the definition of an electronic signature, this could be any data attached to, incorporated in or logically associated with other data which is intended by the user to serve as a signature, such as the user’s name or IP address.

In the absence of any law requiring a signature to a document and in the absence of any agreement between two contracting parties as to the type of electronic signature to be used, it is sufficient if a method to identify the person and his or her approval is used, which has appropriate reliability in the circumstances.

The reader must note that the requirements set out above may be contracted out, in the sense that entities may expressly state that they do not conclude ‘electronic transactions’ and that any agreement or contract which they decide to conclude with another must, in order for it to be legally binding, be reduced to writing in the physical sense and physically signed by a director or owner of the business.

Requirement of originality

The ECTA provides that when any law requires that information has to be retained or presented in its original form, a data message will meet that requirement if the information is capable of being displayed or produced and the integrity thereof has been assessed.

Retention of information

The ECTA stipulates that where it is a legal requirement that information is to be retained, such information may be retained in the form of a data message, provided that such information is accessible for subsequent use, that the original format can be reproduced accurately and that the origin and date when the document was created can be determined.

Formation and validity of contracts and agreements

The ECTA expressly provides that an agreement will not be without legal force merely because it was concluded by electronic means. In other words, where an offer in the form of an email is made and such offer is accepted by return email by the person to whom the offer was made, this will give rise to a transaction or agreement which is legally binding and enforceable. It will give rise to a legal relationship between the two parties which, if not complied with, may be enforced in a court of law.

Furthermore, the ECTA provides that an agreement will be deemed to have been concluded at the time and place where the acceptance of the offer was received by the offeror and that any data message used in the conclusion or performance of an agreement is deemed to have been sent when it enters an information system outside the control of the originator or is capable of being retrieved by the addressee. In other words, any electronic message is deemed to have been received when the complete data message enters an information system designated by the addressee and is capable of being retrieved by the addressee. An acknowledgement of receipt of a data message is not necessary to give effect to that message.

Online trading

The ECTA allows contracts and commercial transactions to be concluded electronically either with a person, a business/company or with an agent, in the form of a computer program acting on behalf of a person or business/company.

ECTA provides certain rights to consumers who transact in such a manner.

For example, a consumer is entitled to cancel, without reason or penalty, any transaction and any related credit agreement for the supply of goods within seven days after the date of receipt of the goods, or for the supply of services within seven days after the conclusion of the agreement.

However, this cooling-off provision does not apply to electronic transactions for financial services, such as to insurance, to banking services, to auctions, to transactions for the supply of foodstuffs, beverages or other goods for consumption, to goods made to the consumer's specifications or to accommodation, catering or leisure services. The cooling-off period is therefore subject to certain exceptions.

In addition, before a transaction can be held to be legally binding and valid, the person transacting with a consumer has to provide the consumer with a vast amount of information, such as the seller or vendor's name and address, its returns or replacement policy should the goods or services be unacceptable or defective, the cooling-off period and terms, the place where the goods or services can be collected or inspected, the price of the goods or services and any exclusions which may apply to the transaction.

Unsolicited mail or SPAM

The ECTA houses a number of provisions which seek to regulate and control the sending of unsolicited emails or spam. It provides that no agreement is concluded where a consumer fails to respond to any unsolicited communication.

The ECTA also provides that when any SPAM is sent, the receiver should be given the opportunity to opt-out, to which the sender must comply in all respects. Certain offences are also created, such as when a person sends unsolicited commercial communications after having been advised that such communications are unwelcome, such sender will be in contravention of the law and liable to a fine or jail time if found guilty.

Where any person sends any unsolicited mail, the receiver has the right to demand from the sender the details as to how it obtained the receiver's email or cell phone data.

Finally, any provision in an agreement which purports to exclude the consumer protection rights as housed under the ECTA will be null and void.

Cybercrime

A variety of computer and cyber-related offences have been created, and provision has been made for the appointment of cyber inspectors in an attempt to deal with computer crime.



WHAT HAPPENS IF YOU DO NOT COMPLY?

Penalties

Non-compliance with the ECTA can give rise to a criminal charge. If such person is found to be guilty as charged, he, she or it will be fined or, if such person is a natural person, sentenced to imprisonment for a period not exceeding five years.

Agreements are binding

In addition to a criminal conviction, an entity may find that it has concluded a legally binding transaction, contract or agreement which it did not intend to conclude or which it had no authority to do. Arguing that one did not know the impact or provisions of the Act will not be permitted as a defense.

Loss of information and evidence

Where information is not correctly retained and archived, the entity may find that such data is lost, or, where incorrectly retained, will be inadmissible in court.



RECOMMENDED ACTIONS OR CONTROLS WHICH SHOULD BE IMPLEMENTED BY THE TARGET AUDIENCE TO ENSURE COMPLIANCE WITH THE ACT

Education and training

- Awareness and training of the ECTA and its relevant provisions which may impact on the business;
- Awareness that transactions done via the internet or on a smart phone or cell phone can create legally binding obligations;
- Awareness of the fact that documents and records can be stored and retained electronically;
- Because a data message constitutes a written agreement, the document needs to be retained in case it has to be referred to at a later stage or used as evidence in a dispute; and
- This will give rise to all entities having to introduce and implement proper archiving and document retention practices across their entire business.

Online trading

- Awareness of legal requirements to be followed when products and services are sold online. Where an individual contracts or trades online, full compliance with the provisions of the Act must be achieved.
- If an entity is to trade online and make use of an automated contracting system, specific attention will have to be given to the system used and the terms attaching to each transaction, which have to be presented to the client and accepted before the transaction can proceed. Certain cooling-off periods in favour of the consumer must be allowed for and the person making use of the system must be assured that the payment process is secure.
- Opt-out procedure provided under all unsolicited electronic communications (SPAM).

FURTHER INFORMATION

Regulator

Department of Communications

Website

www.doc.gov.za