

ECT BILL 2002

To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMME's; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-Government services; and to provide for matters connected therewith.

MEMORANDUM ON THE OBJECTS OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, 2002

SUMMARY

The overall objective of the Bill is to enable and facilitate electronic transactions by creating legal certainty around transactions and communications conducted electronically.

The Bill seeks to address the following policy imperatives:

- * bridging the digital divide by developing a National e-Strategy for South Africa;
- * ensuring legal recognition and functional equivalence between electronic and paper-based transactions;
- * promoting public confidence and trust in electronic transactions; and

- * providing supervision of certain service providers.

Key issues sought to be addressed in the Bill include:

- * Maximising benefits - promotion of universal access, especially for members from previously disadvantaged communities, SMMEs and differently abled people;
- * Legal certainty - providing for the legally-binding effect of electronic transactions and legal recognition of data messages, electronic signatures and electronic evidence;
- * E-government - encouraging electronic communication with government;
- * Security - the registration of cryptography service providers, the accreditation of electronic signature technologies by Authentication Service Providers, and the protection of critical databases;
- * Protection of individuals - protection of the consumer and of privacy as well as the protection of critical data;
- * Illegal activities and enforcement - creation of new "cyber offences" and cyber-inspectors to administer certain provisions;
- * Effective management of Internet-related issues - establishment of a proper management regime with regard to domain names in the Republic and the limitation of liability of Internet Service Providers.

Chapter I: Interpretation, Objects and Application

This part of the Act defines critical words and phrases and sets out the main objects of the Act.

Chapter II: Maximising Benefits and Electronic Policy

The objective is to maximize the benefits the Internet offers by promoting universal and affordable access by all to its possible applications, with a view to bridging the digital divide. The Act requires the development of a national e-Strategy plan by the Minister, in consultation with members of Cabinet. The national e-Strategy plan must include detailed plans and programmes to address the development of a national e-transactions strategy, the promotion of universal access and e-readiness, SMMEs development, empowerment of previously disadvantaged persons and communities, human resource development, contain definable objects and timeframes.

Chapter III: Facilitating Electronic Transactions

This Chapter deals with the removal of legal barriers to electronic transacting. Part 1 provides for the legal recognition to data messages and records. Provision is made for the legal recognition of electronic signatures and "advanced electronic signatures" as a secure form of electronic signing. Electronic data will, subject to certain conditions, be permitted to be retained for statutory record retention purposes; regarded as "writing" a true copy of an "original" record, and provision is made for securing proper evidentiary weight of electronic evidence.

Part 2 deals with the rights and obligations that follow from the communication of data messages, namely contract formation, the time and place of sending and receiving data messages, as well as the time and place where a contract is deemed to have been formed by means of data messages. The Act also provides for the validity of sending notices and other expressions of intent through data messages.

Chapter IV: E-government

This Chapter facilitates electronic filing. It lists the requirements for the production of electronic documents and the integrity of information. Provision is made for a Department or Ministry to accept and transmit documents in the form of electronic data messages, to issue permits or licences in the form of a data message or make or receive payment in electronic form.

Chapter V: Cryptography Providers

The Internet presents security challenges which, without an effective regulatory framework, would pose a threat to the security of consumers and the State. This Chapter requires the suppliers of cryptography materials to register in the prescribed manner their names and addresses, the names of their products and a brief description thereof maintained by the Department of Communications. This will allow investigative authorities such as the SAPS, to identify which organisations provide the encryption technologies, intercepted by them in terms of our monitoring and interception laws. This will enable the investigative authorities to approach these service providers to assist with deciphering the encrypted messages.

Chapter VI: Authentication Service Providers

Identification and authentication of the parties in cyberspace remains a challenge and poses threats to consumers and businesses. The Bill seeks to provide for the establishment of an Accreditation Authority within the Department, allowing voluntary accreditation of electronic signature technologies in accordance with minimum

standards. Once accredited, these "advanced" electronic signatures will allow a party to rely on their authenticity.

Chapter VII: Consumer Protection

Vendors must provide consumers with a minimum set of information, including the price of the product or service, contact details and the right to withdraw from an electronic transaction before its completion. Consumers are also entitled, under certain circumstances, to a "cooling off" period within which they may cancel certain types of transactions concluded electronically without incurring any penalty. Consumers also have the right not to be bound to unsolicited communications (spam) offering goods or services. The Bill also seeks to place the responsibility on businesses trading on-line to make use of sufficiently secure payment systems.

Chapter VIII: Personal Information and Privacy Protection

This Chapter establishes a voluntary regime for protection of personal information. Personal information includes any information capable of identifying an individual. Collectors of personal information (data collectors) may subscribe to a set of universally accepted data protection principles. It is envisaged that consumers will prefer to deal with only those data collectors that have subscribed to the recorded data protection principles. The sanction for breach of these provisions is left to the parties themselves to agree on. Subscription to these principles is voluntary due to the fact that the South African Law Commission is currently developing specific data protection or privacy legislation which is expected to be enacted within 24 months.

Chapter IX: Protection of Critical Data

In terms of its definition, critical data is information which, if compromised, may pose a risk to the national security of the Republic or to the economic or social well being of its citizens. The Minister may prescribe matters relating to the registration of critical databases and require certain procedures and technological methods to be used in their storage and archiving.

Chapter X: Domain Name Authority and Administration

A section 21 company will be established, or an existing one approved, to manage the domain name space of the Republic. Its membership and governance structures must be representative of the general South African society, Government and other stakeholders. The objects, powers and functions of the Authority are provided for in the Bill. Provision is also made for disputes involving domain names to be settled by means of alternative dispute resolution methods. The Minister is empowered to formulate national policy on the .za domain name space.

Chapter XI Limitation of Liability of Service Providers

Chapter XI deals with the limitation of the liability of service providers or so-called "intermediaries" and creates a safe harbour for service providers who are currently exposed to a wide variety of potential liability by virtue of merely fulfilling their basic technical functions. The service providers may seek to limit their liability where they have acted as mere conduits for the transmission of data messages. In each situation the Bill seeks to provide for specific requirements that the actions of the service providers must meet before the clause may be invoked to limit his or her liability.

Chapter XII: Cyber Inspectors

Chapter XII of the Bill seeks to provide for the Department of Communications to appoint cyber inspectors. The cyber inspectors may monitor Internet websites in the public domain and investigate whether cryptography service providers and authentication service providers comply with the relevant provisions. The inspectors are granted powers of search and seizure, subject to obtaining a warrant. Inspectors can also assist the police or other investigative bodies, on request.

Chapter XIII - Cyber Crime

Chapter XIII of the Bill seeks to make the first statutory provisions on cyber crime in South African jurisprudence. The Bill seeks to introduce statutory criminal offences relating to information systems and includes—

- (a) unauthorised access to data;
- (b) interception of or interference with data;
- (c) computer-related extortion;
- (d) fraud; and
- (e) forgery.

Any person aiding or abetting another in the performance of any of these crimes will be guilty as an accessory. The Bill seeks to prescribe the penalties for those convicted of offences.

FINANCIAL IMPLICATIONS

The Bill will lead to new responsibilities for the Department of Communications and to

the development of new infrastructure and systems. Consequently increased financial resources are needed. It will be necessary to equip the required personnel with new skills and proper training especially for technical staff, enabling them to perform the tasks stipulated in the Bill, such as the development and implementation of a National e-Strategy plan.

It is anticipated that the Bill will result in changes to certain laws, which may require a review of laws by other Departments. However, the Bill does not oblige Government departments to accept or issue documents in electronic form. It merely permits departments to do so. In some instances, such as the establishment of Cyber Inspectors, the Accreditation Authority and Cryptography, the Department will require re-organisation and restructuring. This would have definite financial implications for the State. However, the Bill will probably effect an increase in the revenue collected by the Department in the form of fees payable for the accreditation of authentication service providers.

OTHER DEPARTMENTS / AGENCIES CONSULTED

The development of the Bill arose out of a lengthy policy-formulation process resulting in a Discussion Paper and Green Paper on Electronic Commerce. This process included extensive consultations with Government departments and other stakeholders across the spectrum. Following the conclusion of this consultative process, a legal team comprising of consultants, legal practitioners and academics was appointed. This team, together with officials of the Department, and in consultation with other departments, developed the Bill.

Extensive consultative processes were followed in the development of the Bill:

- * An E-Law Conference for all stakeholders was held on 20-21 April 2000;
- * An Interdepartmental Workshop to discuss first draft of the Bill was held on 8 May 2001. All Departments were invited and the following Departments were represented:
 - o Department of Justice;
 - o South African Law Commission;
 - o Department of Agriculture and Land Affairs;
 - o Department of Foreign Affairs;
 - o Government Communication Information System (GCIS);
 - o Department of Education;
 - o State Information Technology Agency (SITA);
 - o Department of Home Affairs;
 - o Department of Trade and Industry;
 - o Department of Environmental Affairs and Tourism;
 - o Department of Public Services and Administration;
 - o Department of Health;
 - o National Development Agency;
 - o Department of Water Affairs and Forestry;
 - o Department of Provincial and Local Government;
 - o South African Reserve Bank;
 - o Department of Labour;
- * The draft Bill was sent to all Directors-General of departments for comments;

* Bilateral meetings were held with the following departments to discuss specific issues:

- o Department of Trade and Industry;
- o Department of Labour.

PARLIAMENTARY PROCEDURE

The Department of communications and the State Law Advisers are of the opinion that the Bill must be dealt with in accordance with the procedure established by section 75 of the Constitution of the Republic since it contains no provision to which the procedure set out in section 74 or 76 of the Constitution applies.

ARRANGEMENT OF SECTIONS

Sections

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

1. Definitions
2. Objects of Act

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-Strategy

5. National e-Strategy
6. Universal access
7. Previously disadvantaged persons and communities
8. Human resources development
9. SMMEs

Part 2

Electronic transactions policy

10. Electronic transactions policy

CHAPTER III

FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

11. Legal recognition of data messages
12. Writing
13. Signature
14. Original
15. Admissibility and evidential weight of data messages
16. Retention
17. Production of document or information
18. Notarisation, acknowledgment and certification
19. Other requirements
20. Certain other legislation not affected
21. Automated transactions

Part 2

Communication of data messages

22. Variation by agreement between parties
23. Formation and validity of agreements
24. Time and place of communications, dispatch and receipt
25. Expression of intent or other statement
26. Attribution of data messages to originator
27. Acknowledgement of receipt of data message

CHAPTER IV

E-GOVERNMENT

28. Acceptance of electronic filing and issue of documents
29. Requirements may be specified

CHAPTER V

CRYPTOGRAPHY PROVIDERS

30. Register of cryptography providers
31. Registration with Department
32. Restrictions on disclosure of information
33. Application of Chapter and offences

CHAPTER VI

AUTHENTICATION SERVICE PROVIDERS

Part 1

Accreditation authority

34. Definitions
35. Appointments of Authority and other officers

CHAPTER VII

CONSUMER PROTECTION

43. Scope of application
44. Information to be provided
45. Cooling off period
46. Unsolicited goods, services or communications

CHAPTER I
INTERPRETATION, OBJECTS AND APPLICATION

Definitions

1. In this Act, unless the context indicates otherwise—

"addressee" of a data message means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;

"advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 38;

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

"authentication service provider" means a person whose authentication products or services have been accredited by the Authority under section 38 or recognised under section 41;

"Authority", for purposes of—

(a) Chapter VI, means the Director-General acting as the Accreditation Authority as provided for in that Chapter;

(b) Chapter X, means the .za domain name space Authority established by that Chapter;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment;

Objects of Act

2. (1) The objects of this Act are to enable and facilitate electronic transactions in the public interest, and for that purpose to—

- (a) recognise the importance of the information economy to the future economic and social prosperity of the Republic;
- (b) promote universal access;
- (c) promote the understanding, acceptance and growth in the number of electronic transactions in the Republic;
- (d) remove and prevent barriers to electronic transactions in the Republic;
- (e) promote legal certainty and confidence in respect of electronic transactions;
- (f) promote technology neutrality in the application of legislation to electronic transactions;
- (g) promote e-Government services and electronic transactions with public and private bodies and institutions;
- (h) ensure that electronic transactions in the Republic conform to the highest international standards;
- (i) encourage investment and innovation in respect of electronic transactions in the Republic;

- (j) develop a safe, secure and effective environment for the consumer, business and Government to conduct and use electronic transactions;
- (k) promote the development of electronic transactions services which are responsive to the needs of users and consumers;
- (l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities, areas and the disabled are duly taken into account;
- (m) ensure compliance with accepted technical standards in the provision and development of electronic transactions;
- (n) promote the stability of electronic transactions in the Republic;
- (o) promote the development of human resources in the electronic transactions environment;
- (p) promote SMMEs within the electronic transactions environment;
- (q) ensure efficient use and management of the .za domain name space; and
- (r) ensure that the national interest of the Republic is not compromised through the use of electronic communications.

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-strategy

National e-Strategy

5. The Minister must, within 24 months after the promulgation of this Act, develop a five-year national e-Strategy for the Republic, which must be submitted to the Cabinet for approval.

Universal access

6. In respect of universal access, the national e-Strategy must outline strategies and programmes to—

- (a) provide Internet connectivity to disadvantaged communities;
 - (b) encourage the private sector to initiate schemes to provide universal access;
 - (c) foster the adoption and use of new technologies for attaining universal access;
- and
- (d) stimulate public awareness, understanding and acceptance of the benefits of Internet connectivity and electronic transacting.

Previously disadvantaged persons and communities

7. The Minister, in developing the national e-Strategy, must provide for ways

of maximising the benefits of electronic transactions for historically disadvantaged persons and communities, including, but not limited to—

- (a) making facilities and infrastructure available or accessible to such persons and communities to enable the marketing and sale of their goods or services by way of electronic transactions;
- (b) providing or securing support services for such facilities and infrastructure to assist with the efficient execution of electronic transactions; and
- (c) rendering assistance and advice to such persons and communities on means to efficiently adopt and utilise electronic transactions.

Human resources development

8. (1) The Minister, in developing national e-strategy, must provide for ways of promoting human resources development set out in this section within the context of the Government's integrated human resource development strategies, having regard to structures and programmes that have been established under existing laws.

(2) The Minister must consult with the Ministers of Labour and Education on existing facilities, programmes and structures for education, training and human resource development in the information technology sector relevant to the objects of this Act.

(3) Subject to subsection (1) and (2), the Minister must promote skills development in the areas of—

- (a) information technology products and services in support of electronic transactions;

- (b) business strategies for SMMEs and other businesses to utilise electronic transactions;
- (c) sectoral, regional, national, continental and international policy formulation for electronic transactions;
- (d) project management on public and private sector implementation of electronic transactions;
- (e) the management of the .za domain name space;
- (f) the management of the IP address system for the African continent in consultation with other African states;
- (g) convergence between communication technologies affecting electronic transactions;
- (h) technology and business standards for electronic transactions;
- (i) education on the nature, scope, impact, operation, use and benefits of electronic transactions; and
- (j) any other matter relevant to electronic transactions as the Minister regards as proper.

SMMEs

9. The Minister must, in consultation with the Minister for Trade and Industry, evaluate the adequacy of any existing processes, programmes and infrastructure providing for the utilisation by SMMEs of electronic transactions and, pursuant to such evaluation and, may—

- (a) establish or facilitate the establishment of electronic communication centres for

SMMEs;

- (b) facilitate the development of websites or website portals that will enable SMMEs to transact electronically and obtain information about markets, products and technical assistance; and
- (c) facilitate the provision of such professional and expert assistance and advice to SMMEs on means to efficiently adopt and utilise electronic transacting for their development.

Part 2

Electronic transactions policy

Electronic transactions policy

10. (1) The Minister must, subject to the provisions of this Act, formulate electronic transactions policy.

(2) In formulating the policy contemplated in subsection (1), the Minister must—

- (a) act in consultation with members of the Cabinet directly affected by such policy formulation or the consequences thereof;
- (b) have due regard to—
 - (i) the objects of this Act;
 - (ii) the nature, scope and impact of electronic transactions;
 - (iii) international best practice and conformity with the law and guidelines of other jurisdictions and international bodies; and

(iv) existing laws and their administration in the Republic.

(3) The Minister must publish policy guidelines in the *Gazette* on such issues as he or she deems relevant to electronic transactions in the Republic.

(4) The Minister may not publish policy guidelines that impose obligations on any person.

CHAPTER III

FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

Legal recognition of data messages

11. (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

(2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.

(3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is—

(a) referred to in a way in which a reasonable person would have noticed the reference to and incorporation thereof; and

(b) accessible in a form in which it may be read, stored and retrieved by the other

party, whether electronically or as a computer printout: Provided such information is reasonably capable of being reduced to electronic form by the party incorporating it.

Writing

12. A requirement under law that a document or information be in writing is met if the document or information is—

- (a) in the form of a data message; and
- (b) accessible in a manner usable for subsequent reference.

Signature

13. (1) Where the signature of a person is required by law, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1) an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) 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, that requirement is met in relation to a data message if:

- (a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
- (b) having regard to all the relevant circumstances at the time the method was used,

the method was as reliable as was appropriate for the purposes for which the information was communicated.

(4) Where an advanced electronic signature has been used, such signature is regarded as having created a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Subsection (4) does not preclude any person from—

- (a) establishing the validity of an advanced electronic signature in any other way; or
- (b) adducing evidence of the non-validity of an advanced electronic signature.

Original

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if—

- (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2) ; and
- (b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a) the integrity must be assessed—

- (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
- (b) in the light of the purpose for which the information was generated; and

- (c) having regard to all other relevant circumstances.

Admissibility and evidential weight of data messages

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence—

- (a) on the mere grounds that it is constituted by a data message; or
- (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to—

- (a) the reliability of the manner in which the data message was generated, stored or communicated;
- (b) the reliability of the manner in which the integrity of the data message was maintained;
- (c) the manner in which its originator was identified; and
- (d) any other relevant factor.

Retention

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if—

- (a) the information contained in the data message is accessible so as to be useable for subsequent reference;
- (b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- (c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Production of document or information

17. (1) Subject to section 29, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, if—

- (a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and
- (b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be useable for subsequent reference;

(2) For the purposes of subsection (1), the integrity of the information

contained in a document is maintained if the information has remained complete and unaltered, except for—

- (a) the addition of any endorsement; or
- (b) any immaterial change,

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

Notarisation, acknowledgment and certification

18. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified, or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

Other requirements

19. (1) A requirement under a law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect must, be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

Certain other legislation not affected

20. This Act does not limit the operation of any law that expressly authorizes, prohibits or regulates the use of data messages, including any requirement by or under a law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method.**Automated transactions**

21. In an automated transaction—

- (a) an agreement may be formed where an electronic agent performs an action required by law for agreement formation;
- (b) an agreement may be formed where all parties to a transaction or either one of them uses an electronic agent;
- (c) a party using an electronic agent to form an agreement is, subject to paragraph (d), bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement.
- (d) a party using an electronic agent to form an agreement is not bound by the terms of that agreement unless those terms were capable of being reviewed by a natural person prior to agreement formation;
- (e) no agreement is formed where a natural person interacts directly with the electronic agent of another person made a material error during the creation of a data message and—
 - (i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;
 - (ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;

- (iii) that person takes reasonable steps, including steps that conform to the other person's instructions to return the performance received, if any, as a result of the error or, if instructed to do so, to destroy that performance; and
- (iv) that person has not used or received any material benefit or value from the performance, if any, received from the other person.

Part 2

Communication of data messages

Variation by agreement between parties

22. This Part only applies if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for in that part.

Formation and validity of agreements

23. (1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.

(2) An agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offerer.

Time and place of communications, dispatch and receipt

24. A data message—

- (a) used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee;
- (b) must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee; and
- (c) must be regarded as having been sent from the originator's usual place of business and as having been received at the addressee's usual place of business.

Expression of intent or other statement

25. As between the originator and the addressee of a data message an expression of intent or other statement is not without legal force and effect merely on the grounds that—

- (a) it is in the form of a data message; or
- (b) it is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred.

Attribution of data messages to originator

- 26.** A data message is that of the originator if it was sent by—
- (a) the originator personally;
 - (b) a person who had authority to act on behalf of the originator in respect of that data message; or
 - (c) an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgement of receipt of data message

27. (1) An acknowledgement of receipt of a data message is not necessary to give legal effect to that message.

- (2) An acknowledgement of receipt may be given by—
- (a) any communication by the addressee, automated or otherwise; or
 - (b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

CHAPTER IV
E-GOVERNMENT

Acceptance of electronic filing and issue of documents

28. Any public body that, pursuant to any law—

- (a) accepts the filing of documents, or requires that documents be created or retained;
- (b) issues any permit, licence or approval; or
- (c) provides for a manner of payment,

may, notwithstanding anything to the contrary in such law—

- (i) accept the filing of such documents, or the creation or retention such documents in the form of data messages;
- (ii) issue such permit, licence or approval in the form of a data message; or
- (iii) make or receive payment in electronic form or by electronic means.

Requirements may be specified

29. In any case where a public body decides to perform any of the functions referred to in section 28, such body may specify by notice in the *Gazette*—

- (a) the manner and format in which the data messages must be filed, created, retained or issued;
- (b) in cases where the data message has to be signed, the type of electronic signature required;

- (c) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message;
- (d) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message;
- (e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and
- (f) any other required attributes for data messages or payments.

CHAPTER V

CRYPTOGRAPHY PROVIDERS

Register of cryptography providers

30. (1) The Director-General must establish and maintain a register of cryptography providers.

(2) The Director-General must record the following particulars in respect of a cryptography provider in the that register:

- (a) The name and address of the cryptography provider;
- (b) a description of the type of cryptography service or cryptography product being provided; and
- (c) such other particulars as may be prescribed to adequately identify and locate the cryptography provider or its products or services.

(3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.

Registration with Department

31. (1) No person may provide cryptography services or cryptography products in the Republic until the particulars referred to in section 30 (2) in respect of that person have been recorded in the register contemplated in section 30 (1).

(2) A cryptography provider must in the prescribed manner furnish the Director-General with the information required and pay the prescribed administrative fee.

(3) A cryptography service or cryptography product is regarded as being provided in the Republic if it is provided—

- (a) from premises in the Republic;
- (b) to a person who is present in the Republic when that person makes use of the service or product; or
- (c) to a person who uses the service or product for the purposes of a business carried on in the Republic or from premises in the Republic.

Restrictions on disclosure of information

32. (1) Information contained in the register provided for in section 30 must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register.

(2) Subsection (1) must not apply in respect of information which is disclosed—

- (a) to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings;
- (b) to government agencies responsible for safety and security in the Republic, pursuant to an official request;
- (c) to a cyber inspector;
- (d) pursuant to sections 11 and 30 of the Promotion of Access to Information Act, 2000; or
- (e) for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

Application of chapter and offences

33. (1) The provisions of this chapter do not apply to the National Intelligence Agency established in terms of section 3 of the Intelligence Services Act, 1994 (Act No. 38 of 1994).

(2) A person who contravenes or fails to comply with a provision of this Chapter is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.

CHAPTER VII
CONSUMER PROTECTION

Scope of application

- 43.** (1) This Chapter applies only to electronic transactions.
- (2) Section 45 does not apply to an electronic transaction—
- (a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;
 - (b) by way of an auction;
 - (c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer.
 - (d) for services which has begun with the consumer's consent before the end of the seven day period referred to in section 45(1);
 - (e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;
 - (f) where the goods—
 - (i) are made to the consumer's specifications;
 - (ii) or clearly personalized;
 - (iii) by reason of their nature cannot be returned; or
 - (iv) are liable to deteriorate or expire rapidly;
 - (g) where audio or video recordings or computer software were unsealed by the

consumer;

- (h) for the sale of newspapers, periodicals and magazines ;
- (i) for the provision of gaming and lottery services; or
- (j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

Information to be provided

44. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the following information available to consumers on the web site where such goods or services are offered:

- (a) Its full name and legal status;
- (b) its physical address and telephone number;
- (c) its web site address and e-mail address;
- (d) membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;
- (e) any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;
- (f) in the case of a legal person, its registration number, the names of its office bearers and its place of registration;
- (g) the physical address where that supplier will receive legal service of documents;
- (h) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on

- the proposed electronic transaction;
- (i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;
 - (j) the manner of payment;
 - (k) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;
 - (l) the time within which the goods will be dispatched or delivered or within which the services will be rendered;
 - (m) the manner and period within which consumers can access and maintain a full record of the transaction;
 - (n) the return, exchange and refund policy of that supplier;
 - (o) any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;
 - (p) the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;
 - (q) where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently; and
 - (r) the rights of consumers in terms of section 45, where applicable.

(2) The supplier must provide a consumer with an opportunity—

- (a) to review the entire electronic transaction;
- (b) to correct any mistakes; and
- (c) to withdraw from the transaction,

before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled in terms of subsection (3)—

- (a) the consumer must return the performance of the supplier or, where applicable, cease using the services performed; and
- (b) the supplier must refund all payment made by the consumer minus the direct cost of returning the goods.

(5) The supplier must utilize a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

Cooling off period

45. (1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply—

- (a) of goods within seven days after the date of the receipt of the goods; or
- (b) of services within seven days after the date of the conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a

consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment which refund must be made within 30 days of the date of cancellation.

(4) This section must not be construed as prejudicing the rights of a consumer provided for by or under any other law.

Unsolicited goods, services or communications

46. (1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer—

- (a) with the option to cancel his or her subscription to the mailing list of that person;
and
- (b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication .

Performance

47. (1) The supplier must execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise .

(2) Where a supplier has failed to execute the order within 30 days , the consumer may cancel the agreement with seven days written notice.

(3) If a supplier is unable to perform in terms of the agreement on the

grounds that the goods or services ordered are unavailable, the supplier must notify the consumer of this fact and refund any payments the consumer has made within 30 days after the date of such notification.

CHAPTER IX

PROTECTION OF CRITICAL DATABASES

Scope of critical database protection

53. The provisions of this Chapter must only apply to a critical database administrator and critical databases or parts thereof.

Identification of critical data and critical databases

- 54.** The Minister may by notice in the *Gazette*—
- (a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data for the purposes of this Chapter; and
 - (b) establish procedures to be followed in the identification of critical databases for the purposes of this Chapter.

Registration of critical databases

- 55.** (1) The Minister may by notice in the *Gazette* determine—
- (a) requirements for the registration of critical databases with the Department or such other body as the Minister may specify;
 - (b) procedures to be followed for registration; and
 - (c) any other matter relating to registration.

(2) For purposes of this Chapter, registration of a critical database means recording the following information in a register maintained by the Department or by such other body as the Minister may specify—

- (a) The full name, address and contact details of the critical database administrator;
- (b) the location of the critical database, including the locations of component parts thereof where a critical database is not stored at a single location; and
- (c) a general description of the categories or types of information stored in the critical database.