Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID-AFRIKA

Vol. 446 Cape Town, Kaapstad, 2 August Augustus 2002 **No. 23708**

THE PRESIDENCY

No. 1046 2 August 2002

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:—

No. 25 of 2002: Electronic Communications and Transactions Act, 2002.

DIE PRESIDENSIE

No. 1046 2 Augustus 2002

Hierby word bekend gemaak dat die President sy goedkeuring geheg het aan die onderstaande Wet wat hierby ter algemene inligting gepubliseer word:—

No. 25 van 2002: Wet op Elektroniese Kommunikasie en Transaksies, 2002.

9 771682 584003 23708

(English text signed by the President.)
(Assented to 31 July 2002.)

ACT

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 SMMEs; 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.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:—

ARRANGEMENT OF SECTIONS

Sections

(Engelse teks deur die President geteken.)
(Goedgekeur op 31 Julie 2002.)

WET

Om voorsiening te maak vir die vergemakliking en regulering van elektroniese kommunikasies en transaksies; om voorsiening te maak vir die ontwikkeling van 'n nasionale e-strategie vir die Republiek; om universele toegang tot elektroniese kommunikasies en transaksies en die gebruik van elektroniese transaksies deur KMMO's te bevorder; om voorsiening te maak vir mensehulpbrononontwikkeling met betrekking tot elektroniese transaksies; om misbruik van inligtingstelsels te verhinder; om die gebruik van e-regeringsdienste aan te moedig; en om voorsiening te maak vir verwante aangeleenthede.

DAAR WORD BEPAAL deur die Parlement van die Republiek van Suid-Afrika, soos volg:—

INDELING VAN ARTIKELS

Artikels

CHAPTER III

FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

Part 2

Communication of data messages

CHAPTER IV

E-GOVERNMENT SERVICES

CHAPTER V

CRYPTOGRAPHY PROVIDERS

CHAPTER VI

AUTHENTICATION SERVICE PROVIDERS

Part 1

Accreditation Authority

HOOFSTUK III

VERGEMAKLIKING VAN ELEKTRONIESE TRANSAKSIES

Deel 1

Regsvereistes vir databoodskappe

Deel 2

Kommunikering van databoodskappe

HOOFSTUK IV

E-REGERINGSDIENSTE

HOOFSTUK V

KRIPTOGRAFIEVERSKAFFERS

HOOFSTUK VI

WAARMERKINGSDIENSVERSKAFFERS

Deel 1

Akkreditasie-owerheid

CHAPTER XIV

GENERAL PROVISIONS

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

Definitions

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

"addressee", in respect 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 37;

"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 Accreditation Authority under section 37 or recognised under section 40;

"Authority" means the .za Domain Name Authority;

"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;

"browser" means a computer program which allows a person to read hyperlinked data messages;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;

"ccTLD" means country code domain at the top level of the Internet's domain name system assigned according to the two-letter codes in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision);

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message;

"consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"Consumer Affairs Committee" means the Consumer Affairs Committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act, 1988 (Act No. 71 of 1988);

"critical data" means data that is declared by the Minister in terms of section 53 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens;

"critical database" means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted;

"critical database administrator" means the person responsible for the management and control of a critical database;

HOOFSTUK XIV

ALGEMENE BEPALINGS

HOOFSTUK I

UITLEG, OOGMERKE EN TOEPASSING

Woordomskrywing

1. In hierdie Wet, tensy uit die samehang anders blyk, beteken—

"administrateur van kritieke databasis" die persoon verantwoordelik vir die bestuur en beheer van 'n kritieke databasis;

"bewaarplek" die primêre register van die inligting wat deur 'n registrasiekantoor bygehou word;

"data" elektroniese voorstellings van inligting in enige formaat;

"databoodskap" data wat op elektroniese wyse voortgebring, gestuur, ontvang of geberg word, en sluit in—

(a) stem, waar die stem in 'n geoutomatiseerde transaksie gebruik word; en

(b) 'n rekord wat geberg word;

"datakontroleur" 'n persoon wat persoonlike inligting vanaf of ten opsigte van 'n datasubjek versoek, versamel, vergelyk, prosesseer of berg;

"datasubjek" 'n natuurlike persoon van wie of ten opsigte van wie persoonlike inligting na die inwerkingtreding van hierdie Wet versoek, ingesamel, vergelyk, geprosesseer of geberg word;

"Departement" die Departement van Kommunikasiewese;

"derde party" met betrekking tot 'n diensverskaffer, 'n intekenaar op die diensverskaffer se dienste of enige ander gebruiker van die diensverskaffer se dienste of 'n gebruiker van inligtingstelsels;

"deurblaaiprogram" ("browser") 'n rekenaarprogram wat 'n persoon in staat stel om databoodskappe met hiperskakels te lees;

"Direkteur-generaal" die Direkteur-generaal van die Departement;

"domeinnaam" 'n alfa-numeriese benaming wat geregistreer of toegewys is ten opsigte van 'n elektroniese adres op die Internet;

"domeinnaamstelsel" 'n stelsel om domeinname na IP-adresse of ander inligting om te skakel;

"DTP" ("WAP") draadlose toepassingsprotokol, 'n oop internasionale standaard wat deur die "Wireless Application Protocol Forum Limited", 'n maatskappy wat ingevolge die wette van die Verenigde Koninkryk ingelyf is, ontwikkel is vir toepassings wat draadlose kommunikasie gebruik, en sluit Internettoegang vanaf 'n mobiele telefoon in;

"elektroniese agent" 'n rekenaarprogram of 'n elektroniese of ander geoutomatiseerde middel wat onafhanklik gebruik word om 'n handeling te begin of om in die geheel of gedeeltelik op databoodskappe of prestasies in 'n geoutomatiseerde transaksie te reageer;

"elektroniese kommunikasie" 'n kommunikasie deur middel van databoodskappe;

"elektroniese handtekening" data wat aangeheg of geïnkorporeer word by, of logies geassosieer word met ander data en wat deur die gebruiker bedoel is om as 'n handtekening te dien;

"cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—

(a) that such data can be accessed only by relevant persons;

(b) the authenticity of the data;

(c) the integrity of the data; or

(d) that the source of the data can be correctly ascertained;

"cryptography provider" means any person who provides or who proposes to provide cryptography services or products in the Republic;

"cryptography service" means any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;

(b) that the authenticity or integrity of such data or data message is capable of being ascertained;

(c) the integrity of the data or data message; or

(d) that the source of the data or data message can be correctly ascertained;

"cyber inspector" means an inspector referred to in Chapter XII;

"data" means electronic representations of information in any form;

"data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"data message" means data generated, sent, received or stored by electronic means and includes—

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

"Department" means the Department of Communications;

"Director-General" means the Director-General of the Department;

"domain name" means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet;

"domain name system" means a system to translate domain names into IP addresses or other information;

"e-government services" means any public service provided by electronic means by any public body in the Republic;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of data messages;

"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;

"e-mail" means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"home page" means the primary entry point web page of a web site;

"hyperlink" means a reference or link from some point in one data message directing a browser or other technology or functionality to another data message or point therein or to another place in the same data message;

"ICANN" means the Internet Corporation for Assigned Names and Numbers, a California non-profit public benefit corporation established in terms of the laws of the state of California in the United States of America;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;

"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"e-pos" elektroniese pos, 'n databoodskap wat in 'n elektroniese kommunikasie gebruik word, of bedoel is om gebruik te word, as 'n posboodskap tussen die opsteller en die geadresseerde;

"e-regeringsdienste" enige openbare diens wat op elektroniese wyse deur enige openbare liggaam in die Republiek gelewer word;

"geadresseerde", ten opsigte van 'n databoodskap, 'n persoon wat deur die opsteller bedoel is om die databoodskap te ontvang, maar nie 'n persoon wat as tussenganger ten opsigte van daardie databoodskap optree nie;

"geoutomatiseerde transaksie" 'n elektroniese transaksie wat in geheel of gedeeltelik aangegaan of verrig is deur middel van databoodskappe waarin die gedrag of databoodskappe van een party of beide partye nie deur 'n natuurlike persoon hersien word in die gewone loop van sodanige natuurlike persoon se besigheid of werk nie;

"geregistreerde" 'n aansoeker om of houer van 'n domeinnaam;

"gevorderde elektroniese handtekening" 'n elektroniese handtekening wat ontstaan uit 'n proses wat deur die Owerheid geakkrediteer is, soos bepaal in artikel 37;

"hiperskakel" 'n verwysing of skakel vanaf 'n punt in een databoodskap wat 'n deurblaaiprogram of ander tegnologie of funksionaliteit verwys na 'n ander databoodskap of punt daarin, of na 'n ander plek in dieselfde databoodskap;

"IKTNN" ("ICANN") die Internet-korporasie vir Toegewese Name en Nommers, 'n Kaliforniese openbarebelangvereniging sonder winsbejag wat ingevolge die wette van die staat van Kalifornië in die Verenigde State van Amerika in die lewe geroep is;

"inligtingstelsel" 'n stelsel om databoodskappe voort te bring, te stuur, te ontvang, te berg, te vertoon of andersins te prosesseer, en sluit die Internet in;

"inligtingstelseldienste" ook die verskaffing van verbindings, die bedryf van fasiliteite vir inligtingstelsels, die verskaffing van toegang tot inligtingstelsels, die uitsending of roetering van databoodskappe tussen punte wat deur 'n gebruiker gespesifiseer word, en die prosessering en berging van data op die individuele versoek van die ontvanger van die diens;

"Internet" die onderling verbinde stelsel van netwerke wat rekenaars oor die wêreld deur gebruikmaking van die OBP/IP verbind en sluit toekomstige weergawes daarvan in;

"IP-adres" beteken die nommer wat die koppelingspunt van 'n rekenaar of ander toestel met die Internet aanwys;

"kasgeheue" hoë-spoedgeheue wat data vir relatief kort tydperke, onder rekenaarbeheer, berg ten einde versending en prosessering van data te versnel;

"KMMO's" ("SMMEs") Klein, Medium en Mikro Ondernemings soos beoog in die Bylaes by die Kleinsake Ontwikkelingswet, 1996 (Wet No. 102 van 1996);

"kriptografiediens" 'n diens wat gelewer word aan 'n afsender of 'n ontvanger van 'n databoodskap of aan enigeen wat 'n databoodskap berg, en wat ontwerp is om die gebruik van kriptografiese tegnieke te vergemaklik ten einde—

(a) te verseker dat slegs sekere persone toegang tot sodanige data of databoodskap kan verkry of dit in 'n verstaanbare vorm kan plaas;

(b) te verseker dat die egtheid of integriteit van die data of databoodskap vasgestel kan word;

(c) die integriteit van die data of databoodskap te verseker; of

(d) te verseker dat die oorsprong van die data of databoodskap korrek vasgestel kan word;

"kriptografieproduk" 'n produk wat gebruik maak van kriptografiese tegnieke en deur 'n afsender of ontvanger van databoodskappe gebruik word ten einde—

(a) te verseker dat slegs relevante persone toegang tot sodanige data kan verkry;

(b) die egtheid van die data te verseker;

(c) die integriteit van die data te verseker; of

(d) te verseker dat die oorsprong van die data korrek vasgestel kan word;

"kriptografieverskaffer" 'n persoon wat kriptografiese dienste of produkte in die Republiek verskaf of voornemens is om dit te verskaf;

"kritieke data" data wat ingevolge artikel 53 deur die Minister verklaar word van belang vir die beskerming van die nasionale veiligheid van die Republiek of die ekonomiese en maatskaplike welsyn van sy burgers te wees;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

"Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof;

"IP address" means the number identifying the point of connection of a computer or other device to the Internet;

"Minister" means the Minister of Communications;

"originator" means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;

"person" includes a public body;

"personal information" means information about an identifiable individual, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but excludes information about an individual who has been dead for more than 20 years;

"prescribe" means prescribe by regulation under this Act;

"private body" means—

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person,

but not a public body;

"public body" means—

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a power or performing a function in terms of any legislation;

"registrant" means an applicant for or holder of a domain name;

"registrar" means an entity which is licensed by the Authority to update a repository;

"kritieke databasis" 'n versameling kritieke data in elektroniese vorm, waar toegang daartoe verkry kan word, of vanwaar dit gereproduseer of onttrek kan word;

"kuberinspekteur" 'n inspekteur in Hoofstuk XII bedoel;

"lkTVD" ("ccTLD") landskode-topvlakdomein van die Internet se domeinnaamstelsel wat ooreenkomstig die tweeletterkodes in die Internasionale Standaard ISO 3166-1 (Kodes vir Naamvoorstellings van Lande en hul Onderverdeling), toegewys is;

"Minister" die Minister van Kommunikasie;

"OBP/IP" ("TCP/IP") die Oorsendingsbeheerprotokol/Internetprotokol wat deur 'n inligtingstelsel gebruik word om met die Internet te verbind;

"openbare liggaam"—

(a) enige staatsdepartement of administrasie in die nasionale of provinsiale sfeer van regering of enige munisipaliteit in die plaaslike sfeer van regering; of

(b) enige ander funksionaris of instelling wanneer dit—

(i) 'n bevoegdheid uitoefen of plig uitvoer ingevolge die Grondwet, of 'n provinsiale grondwet;

(ii) 'n bevoegdheid uitoefen of 'n werksaamheid verrig ingevolge enige wetgewing;

"opsteller" 'n persoon deur wie, of ten behoewe van wie, 'n databoodskap voorgee om gestuur of voortgebring te wees voor berging, indien wel, maar sluit nie 'n persoon in wat as 'n tussenganger ten opsigte van daardie databoodskap optree nie;

"Owerheid" beteken die .za-Domeinnaamowerheid;

"persoon" ook 'n openbare liggaam;

"persoonlike inligting" inligting aangaande 'n herkenbare individu, met inbegrip van, maar nie beperk nie tot—

(a) inligting wat verband hou met die ras, geslagtelikheid, geslag, swangerskap, huwelikstaat, nasionale, etniese of sosiale herkoms, kleur, seksuele georiënteerdheid, ouderdom, fisiese of geestesgesondheid, welsyn, gestremdheid, godsdiens, gewete, oortuiging, kultuur, taal en geboorte van die individu;

(b) inligting wat verband hou met die opvoeding of die mediese, kriminele of werksgeskiedenis van die individu of inligting in verband met finansiële transaksies waarby die individu betrokke was;

(c) enige identifiserende nommer, simbool, of ander besonderheid wat aan die individu toegeken is;

(d) die adres, vingerafdrukke of bloedgroep van die individu;

(e) die persoonlike menings, beskouings of voorkeure van die individu, behalwe waar dit gaan om 'n ander individu of aangaande 'n voorstel vir 'n toewysing, 'n toekenning of 'n prys wat aan 'n ander individu toegeken staan te word;

(f) korrespondensie wat deur die individu gestuur is wat implisiet of eksplisiet van 'n private en vertroulike aard is of verdere korrespondensie wat die inhoud van die oorspronklike korrespondensie sou openbaar;

(g) die beskouinge of menings van 'n ander individu aangaande die individu;

(h) die beskouinge of menings van 'n ander individu aangaande 'n voorstel vir 'n toewysing, 'n toekenning of 'n prys wat aan die individu gedoen staan te word, maar met uitsluiting van die naam van die ander individu waar dit saam met die beskouinge of menings van die ander individu verskyn; en

(i) die naam van die individu waar dit verskyn tesame met ander persoonlike inligting wat betrekking het op die individu of waar die openbaarmaking van die naam self inligting aangaande die individu sal ontbloot,

maar sluit inligting aangaande 'n individu wat reeds meer as 20 jaar gelede oorlede is, uit;

"private liggaam"—

(a) 'n natuurlike persoon wat enige nering, besigheid of professie bedryf of bedryf het, maar slegs in daardie hoedanigheid;

(b) 'n vennnootskap wat enige nering, besigheid of professie bedryf, of dit bedryf het; of

(c) enige voormalige of bestaande regspersoon,

maar nie 'n openbare liggaam nie.

"registrasiekantoor" 'n entiteit wat deur die Owerheid gelisensieer is om 'n spesifieke subdomein te bestuur en te administreer;

"registrateur" 'n entiteit wat deur die Owerheid gelisensieer is om 'n bewaarplek by te hou;

"registry" means an entity licensed by the Authority to manage and administer a specific subdomain;
"repository" means the primary register of the information maintained by a registry;
"second level domain" means the subdomain immediately following the ccTLD;
"SMMEs" means Small, Medium and Micro Enterprises contemplated in the Schedules to the Small Business Development Act, 1996 (Act No. 102 of 1996);
"subdomain" means any subdivision of the .za domain name space which begins at the second level domain;
"TCP/IP" means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet;
"TLD" means a top level domain of the domain name system;
"third party", in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems;
"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;
"universal access" means access by all citizens of the Republic to Internet connectivity and electronic transactions;
"WAP" means Wireless Application Protocol, an open international standard developed by the Wireless Application Protocol Forum Limited, a company incorporated in terms of the laws of the United Kingdom, for applications that use wireless communication and includes Internet access from a mobile phone;
"web page" means a data message on the World Wide Web;
"web site" means any location on the Internet containing a home page or web page;
"World Wide Web" means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer; and
".za domain name space" means the .za ccTLD assigned to the Republic according to the two-letter codes in the International Standard ISO 3166-1.

Objects of Act

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

(a) recognise the importance of the information economy for the economic and social prosperity of the Republic;
(b) promote universal access primarily in underserviced areas;
(c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;
(d) remove and prevent barriers to electronic communications and transactions in the Republic;
(e) promote legal certainty and confidence in respect of electronic communications and transactions;
(f) promote technology neutrality in the application of legislation to electronic communications and transactions;
(g) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;
(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 the 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 and, areas and the disabled are duly taken into account;

"sertifiseringsdiensverskaffer" 'n persoon wat 'n waarmerkingsproduk of -diens verskaf in die vorm van 'n digitale sertifikaat geheg aan, ingelyf by of logies geassosieer met 'n databoodskap;

"subdomein" enige onderafdeling van die .za-domeinnaamruimte wat op die tweedevlakdomein begin;

"transaksie" 'n transaksie van hetsy 'n kommersiële of nie-kommersiële aard, wat die verskaffing van inligting en e-regeringsdienste insluit;

"tuisblad" die primêre toegangspunt-webbladsy van 'n webwerf;

"tussenganger" 'n persoon wat ten behoewe van 'n ander persoon, hetsy as agent al dan nie, 'n bepaalde databoodskap stuur, ontvang of berg of ander dienste ten opsigte van daardie databoodskap lewer;

"TVD" ("TLD") in topvlakdomein van die domeinnaamstelsel;

"tweedevlakdomein" die subdomein of wat onmiddellik volg onder die lkTVD;

"universele toegang" toegang tot Internetverbinding en elektroniese transaksies deur alle burgers van die Republiek;

"verbruiker" 'n natuurlike persoon wat 'n elektroniese transaksie met 'n verskaffer aangaan of wil aangaan as eindgebruiker van die goedere of dienste wat deur daardie verskaffer aangebied word;

"Verbruikersakekomitee" die Verbruikersakekomitee ingestel deur artikel 2 van die Wet op Verbruikersake (Onbillike Sakepraktyke), 1988 (Wet No. 71 van 1988);

"voorskryf" by regulasie kragtens hierdie Wet voorskryf;

"waarmerkingsprodukte of -dienste" produkte of dienste wat ontwerp is om die houer van 'n elektroniese handtekening aan ander persone te identifiseer;

"waarmerkingsdiensverskaffer" 'n persoon wie se waarmerkingsprodukte of -dienste deur die Akkreditasie-owerheid geakkrediteer is kragtens artikel 37 of erken word kragtens artikel 40;

"webbladsy" 'n databoodskap op die Wêreldwye Web;

"webwerf" enige plek op die Internet wat 'n tuisblad of webbladsy bevat;

"Wêreldwye Web" beteken 'n raamwerk om inligting te lees wat 'n gebruiker toelaat om inligting wat op 'n veraf rekenaar gebêre word op te spoor en toegang daartoe te verkry en om verwysings vanaf een rekenaar te volg na verwante inligting op 'n ander rekenaar;

".za-domeinnaamruimte" die .za-lkTVD wat aan die Republiek toegewys is ooreenkomstig die tweeletterkodes in die Internasionale Standaard ISO 3166-1.

Oogmerke van Wet

2. Die oogmerke van hierdie Wet is om in die openbare belang elektroniese kommunikasie en transaksies moontlik te maak en te vergemaklik, en om vir daardie doel—

(a) die belang van die inligtingsekonomie vir die ekonomiese en maatskaplike voorspoed van die Republiek te erken;

(b) universele toegang te bevorder veral in gebiede wat ondervoorsien is;

(c) begrip vir, aanvaarding van en groei in die getal elektroniese transaksies in die Republiek te bevorder;

(d) versperrings tot elektroniese kommunikasies en transaksies in die Republiek te verwyder en te voorkom;

(e) regsekerheid en vertroue ten opsigte van elektroniese kommunikasies en transaksies te bevorder;

(f) tegnologiese neutraliteit by die toepassing van wetgewing op elektroniese transaksies te bevorder;

(g) e-regeringsdienste en elektroniese kommunikasies en transaksies met openbare en private liggame, instellings en burgers te bevorder;

(h) te verseker dat elektroniese transaksies in die Republiek aan die hoogste internasionale standaarde voldoen;

(i) belegging en innovering ten opsigte van elektroniese transaksies in die Republiek aan te moedig;

(j) 'n veilige, geborge en effektiewe omgewing vir die verbruiker, sakewêreld en die Regering te ontwikkel om elektroniese transaksies te bedryf en te gebruik;

(k) die ontwikkeling van elektroniesetransaksiedienste te bevorder wat gehoor gee aan die behoeftes van gebruikers en verbruikers;

(l) te verseker dat, met betrekking tot die verskaffing van elektroniese-transaksiedienste, die spesiale behoeftes van besondere gemeenskappe en gebiede en van gestremdes behoorlik in ag geneem word;

(m) ensure compliance with accepted International technical standards in the provision and development of electronic communications and 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.

Interpretation

3. This Act must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.

Sphere of application

4. (1) Subject to any contrary provision in this section, this Act applies in respect of any electronic transaction or data message.

(2) This Act must not be construed as—

(a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form; or
(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

(3) The sections of this Act mentioned in Column B of Schedule 1 do not apply to the laws mentioned in Column A of that Schedule.

(4) This Act must not be construed as giving validity to any transaction mentioned in Schedule 2.

(5) This Act does not limit the operation of any law that expressly authorises, 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.

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-strategy

National e-strategy

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

(2) The Cabinet must, on acceptance of the national e-strategy, declare the implementation of the national e-strategy as a national priority.

(3) The Minister, in developing the national e-strategy as envisaged in subsection (1)—

(a) must determine all matters involving e-government services in consultation with the Minister for the Public Service and Administration;
(b) must determine the roles of each person, entity or sector in the implementation of the national e-strategy;
(c) must act as the responsible Minister for co-ordinating and monitoring the implementation of the national e-strategy;
(d) may make such investigations as he or she may consider necessary;

(m) nakoming van aanvaarde internasionale tegniese standaarde by die verskaffing en ontwikkeling van elektroniese kommunikasies en transaksies te verseker;
(n) die stabiliteit van elektroniese transaksies in die Republiek te bevorder;
(o) die ontwikkeling van menslike hulpbronne in die omgewing van elektroniese transaksies te bevorder;
(p) KMMO's binne die omgewing van elektroniese transaksies te bevorder;
(q) effektiewe gebruik en bestuur van die .za-domeinnaamruimte te verseker; en
(r) te verseker dat die nasionale belang van die Republiek nie deur die gebruik van elektroniese kommunikasies in gevaar gestel word nie.

Uitleg

3. Hierdie Wet mag nie so uitgelê word dat dit enige statutêre reg of die gemenereg daarvan uitsluit om toegepas te word op, of om erkenning of akkommodasie te verleen aan elektroniese transaksies, databoodskappe of enige ander aangeleentheid waarvoor in hierdie Wet voorsiening gemaak word nie.

Toepassingsfeer

4. (1) Behoudens enige bepaling tot die teendeel in hierdie artikel, is hierdie Wet van toepassing ten opsigte van enige elektroniese transaksie of databoodskap.

(2) Niks in hierdie Wet word so uitgelê—

(a) dat dit van 'n persoon vereis om enige inligting, dokument of handtekening deur of in elektroniese formaat voort te bring, te kommunikeer, te toon, te prosesseer, te stuur, te ontvang, aan te teken, te behou, te berg of te vertoon nie; of
(b) dat dit 'n persoon verbied om vereistes te stel ten opsigte van die wyse waarop daardie persoon databoodskappe sal aanvaar nie.

(3) Die artikels van hierdie Wet wat in Kolom B van Bylae 1 genoem word, is nie van toepassing op die wette wat in Kolom A van daardie Bylae genoem word nie.

(4) Hierdie Wet moet nie uitgelê word asof dit geldigheid verleen aan enige transaksie wat in Bylae 2 genoem word nie.

(5) Hierdie Wet beperk nie die werking van enige wet wat uitdruklik die gebruik van databoodskappe magtig, verbied of reël nie, met inbegrip van enige vereiste van of ingevolge 'n wet, dat inligting op 'n besondere manier geplaas of vertoon moet word, of dat enige inligting of dokument op 'n besondere wyse versend moet word.

HOOFSTUK II

MAKSIMERING VAN VOORDELE EN BELEIDSRAAMWERK

Deel 1

Nasionale e-strategie

Nasionale e-strategie

5. (1) Die Minister moet binne 24 maande na die promulgering van hierdie Wet 'n driejaar- nasionale e-strategie vir die Republiek ontwikkel, wat aan die Kabinet vir goedkeuring voorgelê moet word.

(2) Die Kabinet moet, by aanvaarding van die nasionale e-strategie, die implementering van die nasionale e-strategie tot 'n nasionale prioriteit verklaar.

(3) Die Minister, by die ontwikkeling van die nasionale e-strategie soos beoog in subartikel (1)—

(a) moet alle sake in verband met e-regeringsdienste bepaal in oorleg met die Minister vir die Staatsdiens en Administrasie;
(b) moet die rolle van elke persoon, entiteit of sektor by die implementering van die nasionale e-strategie bepaal;
(c) moet as die verantwoordelike Minister optree om die implementering van die nasionale e-strategie te koördineer en te moniteer;
(d) kan die ondersoeke onderneem wat hy of sy nodig mag ag;

(e) may conduct research into and keep abreast of developments relevant to electronic communications and transactions in the Republic and internationally;

(f) must continually survey and evaluate the extent to which the objectives of the national e-strategy have been achieved;

(g) may liaise, consult and cooperate with public bodies, the private sector or any other person; and

(h) may, in consultation with the Minister of Finance, appoint experts and other consultants on such conditions as the Minister may determine.

(4) *(a)* The Minister must, in consultation with other members of the Cabinet, determine the subject matters to be addressed in the national e-strategy and the principles that must govern the implementation thereof.

(b) Prior to prescribing any subject matter and principles provided for in paragraph *(a)*, the Minister must invite comments from all interested parties by notice in the *Gazette* and consider any comments received.

(c) The national e-strategy must, amongst others, set out—

(i) the electronic transactions strategy of the Republic, distinguishing between regional, national, continental and international strategies;

(ii) programmes and means to achieve universal access, human resource development and development of SMMEs as provided for in this Part;

(iii) programmes and means to promote the overall readiness of the Republic in respect of electronic transactions;

(iv) ways to promote the Republic as a preferred provider and user of electronic transactions in the international market;

(v) existing government initiatives directly or indirectly relevant to or impacting on the national e-strategy and, if applicable, how such initiatives are to be utilised in attaining the objectives of the national e-strategy;

(vi) the role expected to be performed by the private sector in the implementation of the national e-strategy and how government can solicit the participation of the private sector to perform such role;

(vii) the defined objectives, including time frames within which the objectives are to be achieved; and

(viii) the resources required to achieve the objectives provided for in the national e-strategy.

(5) Upon approval by the Cabinet, the Minister must publish the national e-strategy in the *Gazette*.

(6) For purposes of achieving the objectives of the national e-strategy, the Minister may, in consultation with the Minister of Finance—

(a) procure funding from sources other than the State;

(b) allocate funds for implementation of the national e-strategy to such institutions and persons as are responsible for delivery in terms of the national e-strategy and supervise the execution of their mandate; and

(c) take any steps necessary to enable all relevant parties to carry out their respective obligations.

(7) The Minister must annually report to the Cabinet on progress made and objectives achieved or outstanding and may include any other matter the Minister deems relevant.

(8) The Minister must annually review the national e-strategy and where necessary make amendments thereto in consultation with all relevant members of the Cabinet.

(9) No amendment or adaptation of the national e-strategy is effective unless approved by the Cabinet.

(10) The Minister must publish any material revision of the national e-strategy in the *Gazette*.

(11) The Minister must table an annual report in Parliament regarding the progress made in the implementation of the national e-strategy.

Universal access

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

(e) kan navorsing onderneem en op hoogte bly met ontwikkelinge wat verband hou met elektroniese kommunikasies en transaksies in die Republiek en internasionaal;

(f) moet deurentyd die mate waarin die oogmerke van die nasionale e-strategie bereik is, beskou en evalueer;

(g) kan skakel, oorleg pleeg en saamwerk met openbare liggame, die privaatsektor of enige ander persoon; en

(h) kan, in oorleg met die Minister van Finansies, deskundiges en ander konsultante aanstel op die voorwaardes wat die Minister bepaal.

(4) *(a)* Die Minister moet, in oorleg met ander lede van die Kabinet, onderwerpe wat in die nasionale e-strategie behandel moet word, en die beginsels wat die implementering van so 'n onderwerp moet beheer, bepaal;

(b) Voordat enige onderwerp en beginsels waarvoor in paragraaf *(a)* voorsiening gemaak word, voorgeskryf word, moet die Minister by kennisgewing in die *Staatskoerant* kommentaar van alle belanghebbende partye versoek en enige kommentaar wat ontvang word, oorweeg.

(c) Die nasionale e-strategie moet, onder andere, uiteensit—

(i) die elektroniesetransaksiestrategie van die Republiek, met onderskeiding tussen regionale, nasionale, kontinentale en internasionale strategieë;

(ii) programme en middele om universele toegang, mensehulpbronontwikkeling en ontwikkeling van KMMO's waarvoor in hierdie Deel voorsiening gemaak word, te bereik;

(iii) programme en middele om die algehele gereedheid van die Republiek ten opsigte van elektroniese transaksies te bevorder;

(iv) wyses om die Republiek as 'n voorkeurverskaffer en -gebruiker van elektroniese transaksies in die internasionale mark te bevorder;

(v) bestaande regeringsinisiatiewe wat regstreeks of onregstreeks relevant is tot, of 'n invloed het op, die nasionale e-strategie en, indien toepaslik, hoe sulke inisiatiewe gebruik staan te word om die oogmerke van die nasionale e-strategie te bereik;

(vi) die rol wat na verwagting deur die privaatsektor gespeel sal word by die implementering van die nasionale e-strategie, en hoe die regering die deelname van die privaatsektor om sodanige rol te speel, kan versoek;

(vii) die omskrewe doelwitte, met inbegrip van tydsraamwerke waarbinne die oogmerke bereik moet word; en

(viii) die hulpmiddels wat vereis word om die oogmerke te bereik waarvoor in die nasionale e-strategie voorsiening gemaak word.

(5) Na goedkeuring deur die Kabinet moet die Minister die nasionale e-strategie in die *Staatskoerant* publiseer.

(6) Ten einde die oogmerke van die nasionale e-strategie te bereik, kan die Minister, in oorleg met die Minister van Finansies—

(a) finansiering verkry van bronne buiten die staat;

(b) fondse vir die implementering van die nasionale e-strategie toewys aan die instellings en persone wat ingevolge die nasionale e-strategie vir lewering verantwoordelik is, en toesig hou oor die uitvoering van hul mandate; en

(c) die stappe doen wat nodig is om alle betrokke partye in staat te stel om hul onderskeie verpligtinge na te kom;

(7) Die Minister moet jaarliks aan die Kabinet verslag doen oor vordering gemaak en oogmerke bereik of uitstaande en kan hierby insluit enige ander aangeleentheid wat die Minister tersaaklik ag.

(8) Die Minister moet die nasionale e-strategie jaarliks hersien en in oorleg met alle betrokke Kabinetslede, die nodige wysigings aanbring.

(9) Geen wysiging of aanpassing van die nasionale e-strategie is effektief nie, tensy dit deur die Kabinet goedgekeur is.

(10) Die Minister moet enige wesenlike hersiening van die nasionale e-strategie in die *Staatskoerant* publiseer.

(11) Die Minister moet 'n jaarlikse verslag in die Parlement ter tafel lê aangaande die vordering wat met die inwerkingstelling van die nasionale e-strategie gemaak is.

Universele toegang

6. Ten opsigte van universele toegang moet die nasionale e-strategie strategieë en programme uiteensit om—

(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 to 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 ways to adopt and utilise electronic transactions efficiently.

Development of human resources

8. (1) The Minister, in developing the national e-strategy, must provide for ways of promoting development of human resources 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 subsections (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.

SMMEs

9. The Minister must, in consultation with the Minister of 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, may—

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

(a) Internetverbinding aan benadeelde gemeenskappe te verskaf;
(b) die privaatsektor aan te moedig om skemas te begin om universele toegang te verskaf;
(c) die aanneming en gebruik van nuwe tegnologieë vir die bereiking van universele toegang te kweek; en
(d) openbare bewustheid, begrip en aanvaarding van die voordele van Internetverbinding en elektroniese sake doen te stimuleer.

Voorheen benadeelde persone en gemeenskappe

7. By die ontwikkeling van die nasionale e-strategie moet die Minister voorsiening maak vir wyses om die voordele van elektroniese transaksies vir histories benadeelde persone en gemeenskappe te maksimeer, met inbegrip van, maar nie beperk nie tot die—

(a) beskikbaarstelling of toeganklik maak van fasiliteite en infrastruktuur aan sodanige persone en gemeenskappe, om die bemarking en verkoop van hul goedere of dienste deur middel van elektroniese transaksies moontlik te maak;
(b) verskaffing of verkryging van ondersteuningsdienste vir sulke fasiliteite en infrastruktuur om met die effektiewe uitvoering van elektroniese transaksies behulpsaam te wees; en
(c) verlening van bystand en advies aan sulke persone en gemeenskappe oor wyses om elektroniese transaksies effektief aan te neem en te gebruik.

Ontwikkeling van menslike hulpbronne

8. (1) By die ontwikkeling van die nasionale e-strategie moet die Minister voorsiening maak vir wyses om die ontwikkeling van menslike hulpbronne te bevorder, soos in hierdie artikel uiteengesit, binne die raamwerk van die regering se geïntegreerde strategieë vir die ontwikkeling van menslike hulpbronne, met inagneming van strukture en programme wat tot stand gekom het kragtens bestaande wetgewing.

(2) Die Minister moet oorleg pleeg met die Ministers van Arbeid en Onderwys oor bestaande fasiliteite, programme en strukture vir onderwys, opleiding en mensehulpbronontwikkeling in die inligtingstegnologiesektor wat toepaslik is op die oogmerke van hierdie Wet.

(3) Behoudens subartikels (1) en (2) moet die Minister vaardigheidsontwikkeling bevorder op die gebiede van—

(a) inligtingstegnologieprodukte en -dienste ter ondersteuning van elektroniese transaksies;
(b) sakestrategieë vir KMMO's en ander besighede om elektroniese transaksies te gebruik;
(c) sektorale, regionale, nasionale, kontinentale en internasionale beleidsformulering vir elektroniese transaksies;
(d) projekbestuur oor die implementering van elektroniese transaksies deur die openbare en privaatsektor;
(e) bestuur van die .za-domeinnaamruimte;
(f) bestuur van die IP-adresstelsel vir die Afrika-vasteland, in oorleg met ander Afrikastate;
(g) sameloping tussen kommunikasietegnologieë wat elektroniese transaksies raak;
(h) tegnologie en sakestandaarde vir elektroniese transaksies;
(i) onderwys oor die aard, omvang, invloed, bedryf, gebruik en voordele van elektroniese transaksies; en
(j) enige ander aangeleentheid wat elektroniese transaksies raak.

KMMO's

9. Die Minister moet, in oorleg met die Minister van Handel en Nywerheid, die toereikendheid van enige bestaande prosesse, programme en infrastruktuur wat voorsiening maak vir die gebruik van elektroniese transaksies deur KMMO's evalueer, en, na aanleiding van sodanige evaluering, kan—

(a) elektroniese kommunikasiesentrums vir KMMO's instel of die instelling daarvan vergemaklik;

(b) facilitate the development of web sites or web site 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 ways to utilise electronic transacting efficiently for their development.

Part 2

Electronic transactions policy

Electronic transactions policy

10. (1) The Minister must, subject to 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 issues relevant to electronic transactions in the Republic.

(4) In implementing this Chapter, the Minister must encourage the development of innovative information systems and the growth of related industry.

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 thereto 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 as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

Writing

12. A requirement in law that a document or information must 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.

(b) die ontwikkeling van webwerwe of webwerfpoorte vergemaklik wat KMMO's in staat sal stel om elektronies sake te doen en inligting oor markte, produkte en tegniese bystand te verkry; en

(c) die verskaffing vergemaklik van sodanige professionele en deskundige bystand en advies aan KMMO's oor wyses om die doen van elektroniese sake effektief vir hul ontwikkeling te gebruik.

Deel 2

Beleid oor elektroniese transaksies

Beleid oor elektroniese transaksies

10. (1) Die Minister moet, behoudens hierdie Wet, beleid ten opsigte van elektroniese transaksies formuleer.

(2) By die formulering van die beleid in subartikel (1) beoog, moet die Minister—

(a) optree in oorleg met die Kabinetslede wat regstreeks deur sodanige beleidsformulering of die gevolge daarvan geraak word;

(b) behoorlik ag slaan op—

(i) die oogmerke van hierdie Wet;

(ii) die aard, omvang en invloed van elektroniese transaksies;

(iii) internasionale beste praktyk en ooreenstemming met die reg en riglyne van ander jurisdiksies en internasionale liggame; en

(iv) bestaande wetgewing en hul administrasie in die Republiek.

(3) Die Minister moet beleidsriglyne in die *Staatskoerant* publiseer oor vraagstukke wat op elektroniese transaksies in die Republiek van toepassing is.

(4) Met die inwerkingstelling van hierdie Hoofstuk moet die Minister die ontwikkeling van innoverende inligtingstelsels en die groei van aanverwante nywerhede aanmoedig.

HOOFSTUK III

VERGEMAKLIKING VAN ELEKTRONIESE TRANSAKSIES

Deel 1

Regsvereistes vir databoodskappe

Regserkenning van databoodskappe

11. (1) Inligting is nie sonder regskrag of regswerking bloot op grond daarvan dat dit geheel of gedeeltelik in die vorm van 'n databoodskap is nie.

(2) Inligting is nie sonder regskrag of regswerking bloot op grond daarvan dat dit nie vervat is in die databoodskap wat voorgee dat dit aanleiding gee tot die regskrag en regswerking nie, maar slegs na verwys word in sodanige databoodskap.

(3) Inligting wat by 'n ooreenkoms ingelyf is en wat nie in die openbare domein is nie word geag ingelyf te gewees het by 'n databoodskap indien daardie inligting—

(a) na verwys word op 'n wyse waarin 'n redelike persoon die verwysing daarna en inlywing daarvan sou opgemerk het; en

(b) toeganklik is in 'n vorm waarin dit deur die ander party gelees, geberg en herwin kan word, hetsy elektronies of in die vorm van 'n rekenaardrukstuk solank dit vir die party wat dit inlyf redelik moontlik is om die inligting te reduseer tot elektroniese formaat.

Skrif

12. 'n Regsvereiste dat 'n dokument of inligting op skrif moet wees, word nagekom indien die dokument of inligting—

(a) in die vorm van 'n databoodskap is; en

(b) toeganklik is op 'n wyse wat vir latere verwysing bruikbaar is.

Signature

13. (1) 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 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 being a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Where an electronic signature is not required by the parties to an electronic transaction, 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 is evidenced by other means from which such person's intent or other statement can be inferred.

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.

Handtekening

13. (1) Waar die handtekening van 'n persoon regtens vereis word en die regsreël spesifiseer nie die tipe handtekening nie, word aan daardie vereiste met betrekking tot 'n databoodskap voldoen slegs indien 'n gevorderde elektroniese handtekening gebruik word.

(2) Behoudens subartikel (1), is 'n elektroniese handtekening nie sonder regskrag en regswerking bloot op grond daarvan dat dit in elektroniese vorm is nie.

(3) Waar 'n elektroniese handtekening vereis word deur die partye tot 'n elektroniese transaksie en die partye nie ooreengekom het op die tipe elektroniese handtekening wat gebruik moet word nie, word aan hierdie vereiste voldoen ten opsigte van 'n databoodskap indien—

(a) 'n metode gebruik word om die persoon te identifiseer en die persoon se goedkeuring aan te dui van die inligting wat gekommunikeer is; en

(b) in die lig van al die toepaslike omstandighede ten tyde van die gebruik van die metode, die metode so betroubaar was as wat geskik was vir die doeleindes waarvoor die inligting gekommunikeer is.

(4) Waar 'n gevorderde elektroniese handtekening gebruik is, word sodanige handtekening geag 'n geldige elektroniese handtekening te wees en behoorlik toegepas te gewees het, tensy die teendeel bewys word.

(5) Waar 'n elektroniese handtekening nie deur die partye by 'n elektroniese transaksie vereis word nie, is 'n wilsuitdrukking of ander verklaring nie sonder regskrag en regswerking nie bloot op grond daarvan dat—

(a) dit in die vorm van 'n databoodskap is; of

(b) dit nie bewys word deur 'n elektroniese handtekening nie, maar bewys word op 'n ander wyse waarvan so 'n persoon se bedoeling of ander verklaring afgelei kan word.

Oorspronklike

14. (1) Waar 'n wet vereis dat inligting in sy oorspronklike vorm aangebied of behou moet word, voldoen 'n databoodskap aan daardie vereiste indien—

(a) die integriteit van die inligting die toets ingevolge subartikel (2) geslaag het, vanaf die tyd waarop dit vir die eerste keer in sy finale vorm as 'n databoodskap of andersins voortgebring is; en

(b) daardie inligting in staat is om vertoon of voorgelê te word aan die persoon aan wie dit aangebied moet word.

(2) By die toepassing van subartikel (1)*(a)* moet die integriteit beoordeel word—

(a) deur te oorweeg of die inligting volledig en onveranderd gebly het, behalwe vir die byvoeging van enige endossement en enige verandering wat in die normale verloop van kommunikasie, berging en vertoon ontstaan;

(b) in die lig van die doel waarvoor die inligting voortgebring is; en

(c) met inagneming van alle ander toepaslike omstandighede.

Toelaatbaarheid en bewyswaarde van databoodskappe

15. (1) In enige regsgeding mag die reëls van bewysreg nie so aangewend word dat die toelaatbaarheid van 'n databoodskap as getuienis ontken word—

(a) bloot op grond daarvan dat dit 'n databoodskap uitmaak nie; of

(b) indien dit die beste getuienis is wat redelikerwys van die persoon wat dit aanbied verwag kan word om te verkry, op grond daarvan dat dit nie in sy oorspronklike vorm is nie.

(2) Inligting in die vorm van 'n databoodskap moet behoorlike bewyswaarde verleen word.

(3) By die beoordeling van die bewyswaarde van 'n databoodskap, moet oorweging geskenk word aan—

(a) die betroubaarheid van die wyse waarop die databoodskap voortgebring, geberg of gekommunikeer is;

(b) die betroubaarheid van die wyse waarop die integriteit van die databoodskap gehandhaaf is;

(c) die wyse waarop die opsteller daarvan geïdentifiseer is; en

(d) enige ander toepaslike faktor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

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 usable 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 28, 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, and 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 usable 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, acknowledgement 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.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

(4) 'n Databoodskap wat deur 'n persoon in die normale loop van sake gemaak is, of 'n afskrif of drukstuk daarvan, of 'n uittreksel vanuit so 'n databoodskap wat deur 'n ampsdraer in diens van so 'n persoon as korrek gesertifiseer is, is by administratiewe of dissiplinêre verrigtinge ingevolge enige regsreël, die reëls van 'n selfregulerende organisasie, of enige ander wet, of gemenereg, toelaatbaar as getuienis teen enige persoon, en kom neer op weerlegbare bewys van die feite vervat in so 'n rekord, afskrif, drukskrif of uittreksel.

Behoud

16. (1) Waar 'n wet vereis dat inligting behou moet word, word aan daardie vereiste voldoen deur sodanige inligting in die vorm van 'n databoodskap te behou, indien—

(a) die inligting in die databoodskap vervat, toeganklik is sodat dit bruikbaar is vir latere verwysing;

(b) die databoodskap in die formaat is waarin dit voortgebring, gestuur of ontvang is, of in 'n formaat wat bewys kan word die inligting wat voortgebring, gestuur of ontvang is, akkuraat voor te stel; en

(c) die oorsprong en bestemming van daardie databoodskap en die datum en tyd waarop dit gestuur of ontvang is, vasgestel kan word.

(2) Die verpligting om inligting te behou soos beoog in subartikel (1) slaan nie op enige inligting waarvan die uitsluitlike doel is om dit moontlik te maak om die boodskap te stuur of te ontvang nie.

Voorlegging van dokument of inligting

17. (1) Waar 'n wet vereis dat 'n persoon 'n dokument of inligting moet voorlê, word daar behoudens artikel 28 voldoen aan daardie vereiste indien die persoon, deur middel van 'n databoodskap, 'n elektroniese weergawe van daardie dokument of inligting voorlê, en indien—

(a) met inagneming van al die toepaslike omstandighede ten tyde van die afstuur van die databoodskap, die metode van voortbringing van die elektroniese vorm van daardie dokument 'n betroubare wyse gebied het om die behoud van die integriteit van die inligting vervat in daardie dokument te verseker; en

(b) dit ten tyde van die versending van die databoodskap redelik was om te verwag dat die inligting daarin vervat geredelik toeganklik sou wees, sodat dit bruikbaar sou wees vir daaropvolgende verwysing.

(2) By die toepassing van subartikel (1) word die integriteit van die inligting vervat in 'n dokument gehandhaaf indien die inligting volledig en onveranderd gebly het, behalwe vir—

(a) die byvoeging van enige endossement; of

(b) enige onwesenlike verandering wat in die normale verloop van kommunikasie, berging of vertoon ontstaan.

Notarisering, erkenning en sertifisering

18. (1) Waar 'n wet vereis dat 'n handtekening, verklaring of dokument notarieel verly, erken, bewys of onder eed afgelê moet word, word aan daardie vereiste voldoen indien die gevorderde elektroniese handtekening van die persoon wat gemagtig is om daardie handelinge te verrig, aangeheg of ingelyf word by of logies geassosieer word met die elektroniese handtekening of databoodskap.

(2) Waar 'n wet vereis of toelaat dat 'n persoon 'n gesertifiseerde afskrif van 'n dokument of inligting verskaf, en die dokument bestaan in elektroniese vorm, word aan daardie vereiste voldoen indien die persoon 'n drukstuk verskaf wat gesertifiseer is as 'n ware afskrif van die dokument of inligting.

(3) Waar die reg dit vereis of toelaat dat 'n persoon 'n gesertifiseerde afskrif van 'n dokument moet of kan voorsien en die dokument bestaan uit 'n papier- of ander fisiese formaat, word daar aan die vereiste voldoen indien 'n elektroniese afskrif van die dokument gesertifiseer word as 'n ware afskrif en die sertifisering bevestig word deur die gebruik van 'n gevorderde elektroniese handtekening.

Other requirements

19. (1) A requirement in 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.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.

Automated transactions

20. 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)*, presumed to be 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 interacting with an electronic agent to form an agreement is not bound by the terms of the agreement unless those terms were capable of being reviewed by a natural person representing that party prior to agreement formation.

(e) no agreement is formed where a natural person interacts directly with the electronic agent of another person and has 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 any performance received, 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 any performance received from the other person.

Part 2

Communication of data messages

Variation by agreement between parties

21. 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 therein.

Ander vereistes

19. (1) Daar word aan 'n vereiste in 'n wet dat veelvoudige afskrifte van 'n dokument gelyktydig by 'n enkele ontvanger voorgelê moet word, voldoen deur die voorlegging van 'n enkele databoodskap wat deur daardie ontvanger gereproduseer kan word.

(2) 'n Uitdrukking in 'n wet, hetsy as selfstandige naamwoord of werkwoord gebruik, met inbegrip van die uitdrukkings "dokument", "rekord", "aanteken", "indien", "voorlê", "inlewer", "aflewer", "uitreik", "publiseer", "skryf in", "druk" of woorde of uitdrukkings met soortgelyke effek moet uitgelê word sodat dit sodanige vorm, formaat of handeling met betrekking tot 'n databoodskap insluit, tensy andersins daarvoor voorsiening gemaak word in hierdie Wet.

(3) Waar dit regtens vereis word dat 'n seël op 'n dokument aangebring moet word en die regsreël nie die metode of formaat voorskryf waardeur so 'n dokument elektronies verseël moet word nie, word daar aan hierdie vereiste voldoen indien die dokument die vereiste dat dit verseël moet word, aandui en die dokument die gevorderde elektroniese handtekening vervat van die persoon deur wie dit vereis word om verseël te word.

(4) Waar enige regsreël dit vereis of toelaat dat 'n persoon 'n dokument of inligting deur geregistreerde of gesertifiseerde pos of 'n soortgelyke diens, moet of kan stuur, word daar aan hierdie vereiste voldoen indien 'n elektroniese afskrif van die dokument of inligting gestuur word aan die Suid-Afrikaanse Poskantoor Beperk, dit geregistreer word deur genoemde Poskantoor en deur daardie Poskantoor gestuur word aan die elektroniese adres wat deur die afstuurder voorsien word.

Geoutomatiseerde transaksies

20. In 'n geoutomatiseerde transaksie—

(a) kan 'n ooreenkoms gesluit word waar 'n elektroniese agent 'n handeling uitvoer wat regtens vir sluiting van 'n ooreenkoms vereis word;

(b) kan 'n ooreenkoms gesluit word waar al die partye tot 'n transaksie, of enige van hulle, 'n elektroniese agent gebruik;

(c) word 'n party wat 'n elektroniese agent gebruik om 'n ooreenkoms te sluit, behoudens paragraaf *(d)* geag om gebonde te wees aan die bedinge van daardie ooreenkoms, ongeag of daardie persoon die handelinge van die elektroniese agent of die bedinge van die ooreenkoms hersien het;

(d) 'n party wat deur wisselwerking met 'n elektroniese agent 'n ooreenkoms wil sluit, word nie deur die bepalings van die ooreenkoms verbind nie, tensy voor die totstandkoming van die kontrak, daardie bepalings hersien kon word deur 'n natuurlike persoon wat daardie party verteenwoordig.

(e) word geen ooreenkoms gesluit waar 'n natuurlike persoon regstreeks met die elektroniese agent van 'n ander persoon onderhandel en 'n wesenlike fout tydens die skepping van 'n databoodskap gemaak het en—

(i) die elektroniese agent nie aan daardie persoon 'n geleentheid gegee het om die fout te voorkom of reg te stel nie;

(ii) daardie persoon, so gou doenlik nadat daardie persoon dit te wete gekom het, die ander persoon van die fout in kennis stel;

(iii) daardie persoon redelike stappe doen, met inbegrip van stappe wat ooreenstem met die ander persoon se opdragte om enige prestasie wat ontvang is, terug te besorg of daardie prestasie te vernietig, indien aldus gelas; en

(iv) daardie persoon nie enige wesenlike voordeel of waarde gebruik of ontvang het uit enige prestasie wat van die ander persoon ontvang is nie.

Deel 2

Kommunikering van databoodskappe

Wysiging by ooreenkoms tussen partye

21. Hierdie Deel is slegs van toepassing indien die partye wat by die skepping, stuur, ontvangs, berging of andersins by die prosessering van databoodskappe betrokke is nie ooreenkoms bereik het aangaande die kwessies waarvoor daarin voorsiening gemaak word nie.

Formation and validity of agreements

22. (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 offeror.

Time and place of communications, dispatch and receipt

23. 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 or residence and as having been received at the addressee's usual place of business or residence.

Expression of intent or other statement

24. 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

25. 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 unless it is proved that the information system did not properly execute such programming.

Acknowledgement of receipt of data message

26. (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, whether 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 SERVICES

Acceptance of electronic filing and issuing of documents

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

(a) accepts the filing of documents, or requires that documents be created or retained;

Sluiting en geldigheid van ooreenkomste

22. (1) 'n Ooreenkoms is nie sonder regskrag en regswerking bloot omdat dit gedeeltelik of in die geheel deur middel van databoodskappe gesluit is nie.

(2) 'n Ooreenkoms wat deur middel van databoodskappe tussen partye gesluit word, word gesluit op die tyd wanneer en plek waar die aanvaarding van die aanbod deur die aanbieder ontvang word.

Tyd en plek van kommunikasies, versending en ontvangs

23. (1) 'n Databoodskap—

(a) wat by die sluiting van of prestasie ingevolge 'n ooreenkoms gebruik is, moet geag word deur die opsteller gestuur te wees wanneer dit 'n inligtingstelsel buite die beheer van die opsteller binnegaan of, indien die opsteller en geadresseerde in dieselfde inligtingstelsel is, wanneer dit in staat is om deur die geadresseerde herwin te word;

(b) moet geag word deur die geadresseerde ontvang te gewees het wanneer die volledige databoodskap 'n inligtingstelsel binnegaan wat deur die geadresseerde vir daardie doel aangewys of gebruik word en in staat is om deur die geadresseerde herwin of geprosesseer te word; en

(c) moet geag word vanaf die opsteller se gewone besigheidsplek of woning gestuur te gewees het en by die geadresseerde se gewone besigheidsplek of woning ontvang te gewees het.

Betuiging van voorneme of ander verklaring

24. Tussen die opsteller en die geadresseerde van 'n databoodskap is 'n betuiging van voorneme of ander verklaring nie sonder regskrag en regswerking bloot op grond daarvan dat—

(a) dit in die vorm van 'n databoodskap is nie; of

(b) dit nie deur 'n elektroniese handtekening gestaaf word nie maar op ander maniere waaruit die persoon se voorneme of ander verklaring afgelei kan word.

Toeskrywing van databoodskappe aan opsteller

25. 'n Databoodskap word geag dié van die opsteller te wees indien dit—

(a) persoonlik deur die opsteller gestuur is;

(b) gestuur is deur 'n persoon wat magtiging gehad het om ten opsigte van daardie databoodskap namens die opsteller op te tree; of

(c) gestuur is deur 'n inligtingstelsel wat deur of namens die opsteller geprogrammeer is om outomaties te werk tensy dit bewys word dat die inligtingstelsel hierdie programmering nie behoorlik uitgevoer het nie.

Erkenning van ontvangs van databoodskap

26. (1) Geen erkenning van ontvangs van 'n databoodskap is nodig om regswerking aan daardie boodskap te gee nie.

(2) 'n Ontvangserkenning kan gegee word deur middel van—

(a) enige kommunikasie deur die geadresseerde, hetsy outomaties of andersins; of

(b) enige gedrag van die geadresseerde wat voldoende is om aan die opsteller aan te dui dat die databoodskap ontvang is.

HOOFSTUK IV

E-REGERINGSDIENSTE

Aanvaarding van elektroniese indiening en uitreiking van dokumente

27. Enige openbare liggaam wat ooreenkomstig enige wet—

(a) die indiening van dokumente aanvaar of vereis dat dokumente geskep of behou word;

(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 of 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

28. (1) In any case where a public body performs any of the functions referred to in section 27, 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 or that such authentication service provider must be a preferred authentication service provider;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for data messages or payments.

(2) For the purposes of subsection (1)*(d)* the South African Post Office Limited is a preferred authentication service provider and the Minister may designate any other authentication service provider as a preferred authentication service provider based on such authentication service provider's obligations in respect of the provision of universal access.

CHAPTER V

CRYPTOGRAPHY PROVIDERS

Register of cryptography providers

29. (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 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 identify and locate the cryptography provider or its products or services adequately.

(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

30. (1) No person may provide cryptography services or cryptography products in the Republic until the particulars referred to in section 29 in respect of that person have been recorded in the register contemplated in section 29.

(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—

(b) 'n permit, lisensie of goedkeuring uitreik; of

(c) vir 'n wyse van betaling voorsiening maak,

kan, ondanks andersluidende bepalings van sodanige wet—

(i) die indiening van sodanige dokumente, of die skepping of behoud van sodanige dokumente in die vorm van databoodskappe aanvaar;

(ii) sodanige permit, lisensie of goedkeuring in die vorm van 'n databoodskap uitreik; of

(iii) betaling in elektroniese formaat of op elektroniese wyse doen of ontvang.

Vereistes kan vermeld word

28. (1) In enige geval waar 'n openbare liggaam enige van die werksaamhede bedoel in artikel 27 verrig, kan sodanige liggaam by kennisgewing in die *Staatskoerant* die volgende vermeld:

(a) Die wyse waarop en formaat waarin die databoodskappe ingedien, geskep, behou of uitgereik moet word;

(b) in gevalle waar die databoodskap onderteken moet word, die tipe elektroniese handtekening wat vereis word;

(c) die wyse waarop en formaat waarin die elektroniese handtekening aan die databoodskap geheg moet word, daarby ingelyf moet word of andersins daarmee geassosieer moet word;

(d) die identiteit van of kriteria waaraan voldoen moet word deur enige waarmerkingsdiensverskaffer wat gebruik word deur die persoon wat die databoodskap indien of dat so 'n waarmerkingsdiensverskaffer 'n voorkeurdiensverskaffer is;

(e) die toepaslike beheerprosesse en prosedures om voldoende integriteit, veiligheid en vertroulikheid van databoodskappe of betalings te verseker; en

(f) enige ander vereistes vir databoodskappe of betalings.

(2) Vir die doeleindes van subartikel (1)*(d)* is die Suid-Afrikaanse Poskantoor Beperk 'n voorkeurwaarmerkingsdiensverskaffer en kan die Minister enige ander waarmerkingsdiensverskaffer as 'n voorkeurwaarmerkingsdiensverskaffer aanwys, gebaseer op so 'n waarmerkingsdiens se verbintenisse met betrekking tot die verskaffing van universele toegang.

HOOFSTUK V

KRIPTOGRAFIEVERSKAFFERS

Register van kriptografieverskaffers

29. (1) Die Direkteur-generaal moet 'n register van kriptografieverskaffers instel en byhou.

(2) Die Direkteur-generaal moet die volgende besonderhede ten opsigte van 'n kriptografieverskaffer in daardie register aanteken:

(a) Die naam en adres van die kriptografieverskaffer;

(b) 'n beskrywing van die tipe kriptografiediens of kriptografieproduk wat verskaf word; en

(c) die ander besonderhede wat voorgeskryf word om die kriptografieverskaffer of sy of haar produkte of dienste voldoende te identifiseer en op te spoor.

(3) Daar word nie van 'n kriptografieverskaffer verwag om vertroulike inligting of handelsgeheime ten opsigte van sy of haar kriptografieprodukte of -dienste te verskaf nie.

Registrasie by Departement

30. (1) Niemand mag kriptografiedienste of kriptografieprodukte in die Republiek verskaf voordat die besonderhede in artikel 29(2) bedoel ten opsigte van daardie persoon in die register in artikel 29(1) beoog, aangeteken is nie.

(2) 'n Kriptografieverskaffer moet die Direkteur-generaal op die voorgeskrewe wyse voorsien van die inligting wat vereis word en die voorgeskrewe administratiewe gelde betaal.

(3) Daar word geag dat 'n kriptografiediens of kriptografieproduk in die Republiek verskaf word indien dit verskaf word—

(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

31. (1) Information contained in the register provided for in section 29 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) does 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 section 11 or 30 of the Promotion of Access to Information Act, (Act No. 2 of 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

32. (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 VI

AUTHENTICATION SERVICE PROVIDERS

Part 1

Accreditation Authority

Definition

33. In this Chapter, unless the context indicates otherwise—
"accreditation" means recognition of an authentication product or service by the Accreditation Authority.

Appointment of Accreditation Authority and other officers

34. (1) For the purposes of this Chapter the Director-General must act as the Accreditation Authority.

(2) The Accreditation Authority, after consultation with the Minister, may appoint employees of the Department as Deputy Accreditation Authorities and officers.

Accreditation to be voluntary

35. Subject to section 30, a person may, without the prior authority of any other person, sell or provide authentication products or services in the Republic.

Powers and duties of Accreditation Authority

36. (1) The Accreditation Authority may—

(a) vanaf persele in die Republiek;
(b) aan 'n persoon wat in die Republiek aanwesig is wanneer daardie persoon van die diens of produk gebruik maak; of
(c) aan 'n persoon wat die diens of produk gebruik vir die doeleindes van 'n besigheid wat in die Republiek of vanaf persele in die Republiek bedryf word.

Beperkings op openbaarmaking van inligting

31. (1) Inligting wat vervat is in die register waarvoor in artikel 29 voorsiening gemaak word, mag nie openbaargemaak word aan enige ander persoon as werknemers van die Departement wat verantwoordelik is vir die byhou van die register nie.

(2) Subartikel (1) is nie van toepassing nie ten opsigte van inligting wat openbaargemaak word—

(a) aan 'n toepaslike owerheid wat 'n kriminele misdryf ondersoek of vir die doeleindes van enige strafregtelike verrigtinge;
(b) aan regeringsagentskappe wat verantwoordelik is vir veiligheid en sekuriteit in die Republiek, ooreenkomstig 'n amptelike versoek;
(c) aan 'n kuberinspekteur;
(d) ooreenkomstig artikel 11 of 30 van die Wet op Bevordering van Toegang tot Inligting (Wet No. 2 van 2000); of
(e) vir doeleindes van enige siviele verrigtinge wat verband hou met die verskaffing van kriptografiedienste of kriptografieprodukte en waarby 'n kriptografieverskaffer 'n party is.

Toepassing van Hoofstuk en misdrywe

32. (1) Die bepalings van hierdie Hoofstuk is nie van toepassing op die Nasionale Intelligensie-agentskap wat ingestel is ingevolge artikel 3 van die Wet op Intelligensie-dienste, 1994 (Wet No. 38 van 1994), nie.

(2) 'n Persoon wat 'n bepaling van hierdie Hoofstuk oortree of versuim om daaraan te voldoen, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk wat nie twee jaar oorskry nie.

HOOFSTUK VI

WAARMERKINGSDIENSVERSKAFFERS

Deel 1

Akkreditasie-owerheid

Woordomskrywing

33. In hierdie Hoofstuk, tensy die samehang anders aandui, beteken—

"akkreditasie" 'n erkenning van 'n waarmerkingsproduk of -diens deur die Akkreditasie-owerheid.

Aanstelling van Akkreditasie-owerheid en ander beamptes

34. (1) By die toepassing van hierdie Hoofstuk moet die Direkteur-generaal as die Akkreditasie-owerheid optree.

(2) Die Akkreditasie-owerheid kan, na oorleg met die Minister, werknemers van die Departement as Adjunk Akkreditasie-owerhede en beamptes aanstel.

Akkreditasie vrywillig te wees

35. (1) Behoudens artikel 30 kan 'n persoon sonder die voorafgaande magtiging van enige ander persoon waarmerkingsprodukte of -dienste in die Republiek verkoop of verskaf.

Bevoegdhede en pligte van Akkreditasie-owerheid

36. (1) Die Akkreditasie-owerheid kan—

(a) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act;

(b) temporarily suspend or revoke the accreditation of an authentication product or service; and

(c) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act.

(2) The Accreditation Authority must maintain a publicly accessible database in respect of—

(a) authentication products or services accredited in terms of section 37;

(b) authentication products and services recognised in terms of section 40;

(c) revoked accreditations or recognitions; and

(d) such other information as may be prescribed.

Part 2

Accreditation

Accreditation of authentication products and services

37. (1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.

(2) An application for accreditation must—

(a) be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and

(b) be accompanied by a non-refundable prescribed fee.

(3) A person falsely holding out its products or services to be accredited by the Accreditation Authority is guilty of an offence.

Criteria for accreditation

38. (1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—

(a) is uniquely linked to the user;

(b) is capable of identifying that user;

(c) is created using means that can be maintained under the sole control of that user; and

(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;

(e) is based on the face-to-face identification of the user.

(2) For purposes of subsection (1), the Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services:

(a) Its financial and human resources, including its assets;

(b) the quality of its hardware and software systems;

(c) its procedures for processing of products or services;

(d) the availability of information to third parties relying on the authentication product or service;

(e) the regularity and extent of audits by an independent body;

(f) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and

(g) any other relevant factor which may be prescribed.

(3) For the purposes of subsections (2)(*b*) and (*c*), the hardware and software systems and procedures must at least—

(a) be reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability and correct operation;

(a) die optrede, stelsels en werking van 'n waarmerkingsdiensverskaffer moniteer om te verseker dat dit aan artikel 38 en die ander verpligtinge van waarmerkingsdiensverskaffers ingevolge hierdie Wet voldoen;

(b) die akkreditasie van 'n waarmerkingsproduk of -diens tydelik opskort of intrek; en

(c) 'n onafhanklike ouditeursfirma aanstel om periodieke oudits van die waarmerkingsdiensverskaffer te doen om te verseker dat dit aan artikel 38 en die ander verpligtinge van waarmerkingsdiensverskaffers ingevolge hierdie Wet voldoen;

(2) Die Akkreditasie-owerheid moet 'n databasis wat vir die publiek toeganklik is, byhou ten opsigte van—

(a) waarmerkingsprodukte of -dienste wat ingevolge artikel 37 geakkrediteer is;

(b) waarmerkingsprodukte en -dienste wat ingevolge artikel 40 erken word;

(c) akkreditasies of erkennings wat ingetrek is; en

(d) die ander inligting wat voorgeskryf word.

Deel 2

Akkreditasie

Akkreditasie van waarmerkingsprodukte en -dienste

37. (1) Die Akkreditasie-owerheid kan waarmerkingsprodukte of -dienste ter ondersteuning van gevorderde elektroniese handtekeninge akkrediteer.

(2) 'n Aansoek om akkreditasie moet—

(a) op die voorgeskrewe wyse by die Akkreditasie-owerheid gedoen word en gestaaf word deur die voorgeskrewe inligting; en

(b) vergesel gaan van die voorgeskrewe geld, wat nie terugbetaalbaar is nie.

(3) 'n Persoon wat valslik voorgee dat sy of haar produkte of dienste by die Akkreditasie-owerheid geakkrediteer is, is skuldig aan 'n misdryf.

Kriteria vir akkreditasie

38. (1) Die Akkreditasie-owerheid mag nie waarmerkingsprodukte of -dienste akkrediteer nie tensy die Akkreditasie-owerheid oortuig is dat 'n elektroniese handtekening waarop die waarmerkingsprodukte of -dienste betrekking het—

(a) uniek aan die gebruiker gekoppel is;

(b) in staat is om daardie gebruiker te identifiseer;

(c) geskep is deur die gebruik van middele wat onder die uitsluitlike beheer van daardie gebruiker onderhou kan word;

(d) op so 'n wyse aan die data of databoodskap waarop dit betrekking het, gekoppel sal wees dat enige latere verandering van die data of databoodskap opspoorbaar is; en

(e) word gebaseer op die van-aangesig-tot-aangesig identifikasie van die gebruiker.

(2) By die toepassing van subartikel (1) moet die Akkreditasie-owerheid die volgende faktore ten opsigte van 'n waarmerkingsdiensverskaffer in ag neem voor die akkreditering van waarmerkingsprodukte of -dienste:

(a) Die verskaffer se finansiële en menslike hulpbronne, met inbegrip van die bates;

(b) die kwaliteit van die verskaffer se hardeware- en sagtewarestelsels;

(c) die verskaffer se prosedures om produkte of dienste te prosesseer;

(d) die beskikbaarheid van inligting aan derde partye wat op die waarmerkingsproduk of -diens staatmaak;

(e) die gereeldheid en omvang van oudits deur 'n onafhanklike liggaam;

(f) die faktore bedoel in subartikel (4) waar die produkte en dienste deur 'n sertifiseringsdiensverskaffer gelewer word; en

(g) enige ander toepaslike faktor wat voorgeskryf word.

(3) By die toepassing van subartikel (2)*(b)* en *(c)* moet die hardeware- en sagtewarestelsels en prosedures minstens—

(a) redelik beveilig wees teen inmenging en misbruik;

(b) 'n redelike vlak van beskikbaarheid, betroubaarheid en korrekte werking verskaf;

(c) be reasonably suited to performing their intended functions; and

(d) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Accreditation Authority may stipulate, prior to accrediting authentication products or services—

(a) the technical and other requirements which certificates must meet;

(b) the requirements for issuing certificates;

(c) the requirements for certification practice statements;

(d) the responsibilities of the certification service provider;

(e) the liability of the certification service provider;

(f) the records to be kept and the manner in which and length of time for which they must be kept;

(g) requirements as to adequate certificate suspension and revocation procedures; and

(h) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(5) The Accreditation Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service.

Revocation or termination of accreditation

39. (1) The Accreditation Authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40.

(2) Subject to the provisions of subsection (3), the Accreditation Authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1) unless it has—

(a) notified the authentication service provider in writing of its intention to do so;

(b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40; and

(c) afforded the authentication service provider the opportunity to—

(i) respond to the allegations in writing; and

(ii) remedy the alleged breach within a reasonable time.

(3) The Accreditation Authority may suspend accreditation granted under section 38 or recognition given under section 40 with immediate effect for a period not exceeding 90 days, pending implementation of the procedures required by subsection (2), if the continued accreditation or recognition of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in the Republic.

(4) An authentication service provider whose products or services have been accredited in terms of this Chapter may terminate such accreditation at any time, subject to such conditions as may be agreed to at the time of accreditation or thereafter.

Accreditation of foreign products and services

40. (1) The Minister may, by notice in the *Gazette* and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.

(2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1), is guilty of an offence.

Accreditation regulations

41. The Minister may make regulations in respect of—

(a) the rights and obligations of persons relating to the provision of accredited products and services;

(c) redelik geskik wees om hul bedoelde funksies te verrig; en
(d) voldoen aan algemeen aanvaarde sekerheidsprosedures.

(4) By die toepassing van subartikel (1), waar die produkte of dienste deur 'n sertifiseringsdiensverskaffer voorsien word, kan die Akkreditasie-owerheid voor die akkreditering van waarmerkingsprodukte of -dienste bepalings maak oor—

(a) die tegniese en ander vereistes waaraan sertifikate moet voldoen;
(b) die vereistes vir die uitreiking van sertifikate;
(c) die vereistes vir sertifiseringspraktykstate;
(d) die verantwoordelikhede van die sertifiseringsdiensverskaffer;
(e) die aanspreeklikheid van die sertifiseringsdiensverskaffer;
(f) die rekords wat gehou moet word en die wyse waarop en die tydperk waarvoor dit gehou moet word;
(g) vereistes vir voldoende prosedures vir die opskorting en intrekking van sertifikate; en
(h) vereistes oor voldoende kennisgewingsprosedures met betrekking tot die opskorting en intrekking van sertifikate.

(5) Die Akkreditasie-owerheid kan enige nodige voorwaardes of beperkings oplê wanneer 'n waarmerkingsproduk of -diens geakkrediteer word.

Intrekking of beëindiging van akkreditasie

39. (1) Indien die Akkreditasie-owerheid oortuig is dat 'n waarmerkingsdiensverskaffer versuim het of ophou om te voldoen aan enige van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditasie kragtens artikel 38 verleen is of erkenning ingevolge artikel 40 gegee is, kan die Akkreditasie-owerheid die akkreditasie opskort of intrek.

(2) Behoudens die bepalings van subartikel (3) mag die Akkreditasie-owerheid nie die akkreditasie beoog in subartikel (1) opskort of intrek nie, tensy die Akkreditasie-owerheid—

(a) die waarmerkingsdiensverskaffer skriftelik in kennis gestel het van die voorneme om dit te doen;
(b) 'n beskrywing gegee het van die beweerde skending van enige van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditasie kragtens artikel 38 verleen is of erkenning ingevolge artikel 40 gegee is;
(c) aan die waarmerkingdiensverskaffer die geleentheid gegee het om—
  (i) skriftelik op die bewerings te reageer; en
  (ii) die beweerde skending binne 'n redelike tyd reg te stel.

(3) Die Akkreditasie-owerheid kan akkreditasie kragtens artikel 38 verleen of erkenning ingevolge artikel 40 gegee, opskort met onmiddellike werking vir 'n tydperk wat nie 90 dae oorskry nie, hangende implementering van die prosedures wat vereis word deur subartikel (2), indien die volgehoue akkreditasie of erkenning van die waarmerkingdiensverskaffer redelik waarskynlik onherstelbare skade aan verbruikers of aan enige persoon wat by 'n elektroniese transaksie in die Republiek betrokke is, sal veroorsaak.

(4) 'n Waarmerkingsdiensverskaffer wie se produkte of dienste ingevolge hierdie Hoofstuk geakkrediteer is, kan sodanige akkreditasie te eniger tyd beëindig, behoudens die voorwaardes waarop ten tyde van die akkreditasie of daarna ooreengekom word.

Akkreditasie van buitelandse produkte en dienste

40. (1) Die Minister kan, by kennisgewing in die *Staatskoerant* en behoudens die voorwaardes wat deur hom of haar bepaal word, die akkreditasie of soortgelyke erkenning wat aan enige waarmerkingsdiensverskaffer of sy of haar waarmerkingsprodukte of -dienste in 'n buitelandse jurisdiksie verleen is, erken.

(2) 'n Waarmerkingsdiensverskaffer wat valslik voorgee dat sy of haar waarmerkingsprodukte of -dienste deur die Minister ingevolge subartikel (1) erken is, is skuldig aan 'n misdryf.

Regulasies betreffende akkreditasie

41. Die Minister kan regulasies uitvaardig ten opsigte van—

(a) die regte en verpligtinge van persone met betrekking tot die voorsiening van geakkrediteerde produkte en dienste;

(*b*) the manner in which the Accreditation Authority must administer and supervise compliance with those obligations;
(*c*) the procedure pertaining to the granting, suspension and revocation of accreditation;
(*d*) fees to be paid;
(*e*) information security requirements or guidelines; and
(*f*) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Chapter.

CHAPTER VII

CONSUMER PROTECTION

Scope of application

42. (1) This Chapter applies only to electronic transactions.
(2) Section 44 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 began with the consumer's consent before the end of the seven-day period referred to in section 44(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) are clearly personalised;
(iii) by reason of their nature cannot be returned; or
(iv) are likely 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, magazines and books;
(*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.

(3) This Chapter does not apply to a regulatory authority established in terms of a law if that law prescribes consumer protection provisions in respect of electronic transactions.

Information to be provided

43. (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;

(b) die wyse waarop die Owerheid nakoming van daardie verpligtinge moet administreer en kontroleer;
(c) die prosedure wat pas by die verlening, opskorting en intrekking van akkreditasie;
(d) gelde wat betaal moet word;
(e) inligtingsekerheidsvereistes of -riglyne; en
(f) enige ander toepaslike aangeleentheid wat nodig en dienstig is om voor te skryf vir die behoorlike implementering van hierdie Hoofstuk.

HOOFSTUK VII

VERBRUIKERSBESKERMING

Bestek van toepassing

42. (1) Hierdie Hoofstuk is slegs op elektroniese transaksies van toepassing.
(2) Artikel 44 is nie van toepassing nie op 'n elektroniese transaksie—
(a) vir finansiële dienste, met inbegrip van maar nie beperk nie tot, beleggingsdienste, versekerings- en herversekeringsbedrywighede, bankdienste en bedrywighede met betrekking tot handel in effekte;
(b) by wyse van 'n veiling;
(c) vir die lewering van voedsel, drank of ander goedere bedoel vir alledaagse verbruik wat by die huis, verblyfplek of werkplek van die verbruiker gelewer word;
(d) vir dienste wat begin is met die verbruiker se toestemming voor die einde van die tydperk van sewe dae bedoel in artikel 44(1);
(e) waar die prys vir die voorsiening van goedere of dienste afhanklik is van skommelinge in die finansiële markte wat nie deur die voorsiener beheer kan word nie;
(f) waar die goedere—
(i) vervaardig word volgens die verbruiker se spesifikasies;
(ii) duidelik op die persoon afgestem is;
(iii) weens die aard van die goedere nie teruggegee kan word nie;
(iv) geneig is om vinnig te bederf of te verstryk;
(g) waar die verseëling om oudio- of video-opnames of rekenaarsagteware deur die verbruiker gebreek is;
(h) vir die verkoop van koerante, weekblaaie, tydskrifte en boeke;
(i) vir die voorsiening van dobbel- en loterydienste; of
(j) vir die voorsiening van akkommodasie, vervoer, spyseniers- of ontspanningsdienste en waar die leweransier, wanneer die transaksie beklink word, onderneem om hierdie dienste op 'n spesifieke datum of binne 'n spesifieke tydperk te lewer.

(3) Hierdie Hoofstuk is nie van toepassing op 'n regulerende owerheid wat ingevolge 'n regsreël tot stand gebring is nie indien daardie regsreël maatreëls vir verbruikersbeskerming met betrekking tot elektroniese transaksies voorskryf.

Inligting wat verskaf moet word

43. (1) 'n Leweransier wat enige goedere of dienste te koop, te huur of te ruil aanbied by wyse van 'n elektroniese transaksie moet die volgende inligting aan verbruikers beskikbaar stel op die webwerf waar sodanige goedere of dienste aangebied word:
(a) Sy of haar volle naam en regstatus;
(b) sy of haar fisiese adres en telefoonnommer;
(c) sy of haar webwerfadres en e-posadres;
(d) lidmaatskap van enige selfregulerende of akkrediteringsliggame waaraan daardie leweransier behoort of by aangesluit is en die kontakbesonderhede van daardie liggaam;
(e) enige gedragskode wat daardie leweransier onderskryf en hoe die verbruiker elektronies toegang tot daardie gedragskode kan verkry;
(f) in die geval van 'n regspersoon, sy registrasienommer, die name van sy ampsdraers en sy plek van registrasie;
(g) die fisiese adres waar daardie leweransier regsbetekening van dokumente sal ontvang;

(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 44, 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 payments made by the consumer minus the direct cost of returning the goods.

(5) The supplier must utilise 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

44. (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 in any other law.

Unsolicited goods, services or communications

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

(h) 'n voldoende beskrywing van die hoofkenmerke van die goedere of dienste wat deur daardie leweransier aangebied word om 'n verbruiker in staat te stel om 'n ingeligte besluit oor die voorgestelde elektroniese transaksie te neem;

(i) die volle prys wat vir die goedere of dienste betaal moet word, met inbegrip van vervoerkostes, belastings en enige ander gelde of kostes;

(j) die wyse van betaling;

(k) enige bedinge van ooreenkoms, met inbegrip van waarborge, wat op die transaksie van toepassing sal wees, en hoe verbruikers elektronies tot daardie bedinge toegang kan verkry of dit kan berg of reproduseer;

(l) die tydperk waarbinne die goedere versend of afgelewer sal word of waarbinne die dienste gelewer sal word;

(m) die wyse waarop en tydperk waarbinne verbruikers toegang kan verkry tot 'n volledige rekord van die transaksie en dit kan byhou;

(n) die beleid van daardie leweransier oor teruggawe, vervanging en terugbetaling;

(o) enige alternatiewe geskilbeslegtingskode wat daardie leweransier onderskryf en hoe die verbruiker elektronies toegang tot die bewoording van daardie kode kan verkry;

(p) die veiligheidsprosedures en privaatheidsbeleid van daardie leweransier met betrekking tot betaling, betalingsinligting en persoonlike inligting;

(q) waar van toepassing, die minimum duur van die ooreenkoms in die geval van ooreenkomste vir die lewering van produkte of dienste wat op 'n deurlopende grondslag of herhaaldelik uitgevoer moet word; en

(r) die regte van verbruikers ingevolge artikel 44, waar van toepassing.

(2) Die leweransier moet 'n verbruiker 'n geleentheid gee—

(a) om die hele elektroniese transaksie te hersien;

(b) om enige foute reg te stel; en

(c) om aan die transaksie te onttrek, voordat enige bestelling finaal geplaas word.

(3) Indien 'n leweransier versuim om aan die bepalings van subartikel (1) of (2) te voldoen, kan die verbruiker die ooreenkoms kanselleer binne 14 dae na ontvangs van die goedere of dienste kragtens die transaksie.

(4) Indien 'n transaksie gekanselleer word ingevolge subartikel (3)—

(a) moet die verbruiker die prestasie van die leweransier teruggee, of waar van toepassing, ophou om die gelewerde dienste te gebruik; en

(b) moet die leweransier alle betalings wat deur die verbruiker gedoen is, teruggee minus die regstreekse koste om die goedere terug te besorg.

(5) Die leweransier moet 'n betalingstelsel gebruik wat voldoende veilig is met verwysing na aanvaarde tegnologiese standaarde ten tyde van die transaksie en na die tipe transaksie wat betrokke is.

(6) Die leweransier is aanspreeklik vir enige skade wat deur 'n verbruiker gely word as gevolg van 'n versuim deur die leweransier om aan subartikel (5) te voldoen.

Afkoeltydperk

44. (1) 'n Verbruiker is geregtig om sonder rede en sonder strafbeding enige transaksie en enige verwante kredietooreenkoms vir die lewering—

(a) van goedere te kanselleer binne sewe dae na die datum van die ontvangs van die goedere; of

(b) van dienste te kanselleer binne sewe dae na die datum van die sluiting van die ooreenkoms.

(2) Die enigste vordering wat die verbruiker opgelê kan word, is die regstreekse koste om die goedere terug te stuur.

(3) Indien betaling vir die goedere of dienste geskied het voordat 'n verbruiker 'n reg in subartikel (1) bedoel, uitoefen, is die verbruiker geregtig op 'n volledige terugbetaling van sodanige betaling, en die terugbetaling moet geskied binne 30 dae na die datum van kansellasie.

(4) Hierdie artikel mag nie uitgelê word asof dit die regte van 'n verbruiker waarvoor in enige ander wet voorsiening gemaak word, benadeel nie.

Ongevraagde goedere, dienste of kommunikasies

45. (1) Enige persoon wat ongevraagde handelskommunikasies aan verbruikers stuur, moet die verbruiker voorsien—

(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.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

Performance

46. (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 or within the agreed period, 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 immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

Applicability of foreign law

47. The protection provided to consumers in this Chapter, applies irrespective of the legal system applicable to the agreement in question.

Non-exclusion

48. Any provision in an agreement which excludes any rights provided for in this Chapter is null and void.

Complaints to Consumer Affairs Committee

49. A consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of this Chapter by a supplier.

CHAPTER VIII

PROTECTION OF PERSONAL INFORMATION

Scope of protection of personal information

50. (1) This Chapter only applies to personal information that has been obtained through electronic transactions.

(2) A data controller may voluntarily subscribe to the principles outlined in section 51 by recording such fact in any agreement with a data subject.

(3) A data controller must subscribe to all the principles outlined in section 51 and not merely to parts thereof.

(4) The rights and obligations of the parties in respect of the breach of the principles outlined in section 51 are governed by the terms of any agreement between them.

Principles for electronically collecting personal information

51. (1) A data controller must have the express written permission of the data subject

(a) van die opsie om sy of haar intekening op die poslys van daardie persoon te kanselleer: en

(b) op versoek van die verbruiker, van die identifiseringsbesonderhede van die bron waarvandaan daardie persoon die verbruiker se persoonlike inligting gekry het.

(2) Geen ooreenkoms word bereik waar 'n verbruiker versuim het om op 'n ongevraagde kommunikasie te antwoord nie.

(3) Enige persoon wat versuim om te voldoen aan subartikel (1) of dit oortree, is skuldig aan 'n misdryf en is, na skuldigbevinding, strafbaar met die strafmaatreëls wat in artikel 89(1) voorgeskryf word.

(4) Enige persoon wat ongevraagde handelskommunikasies stuur aan 'n persoon wat die afsender in kennis gestel het dat sulke kommunikasies onwelkom is, is skuldig aan 'n misdryf en, na skuldigbevinding, strafbaar met die strafmaatreëls wat in artikel 89(1) voorgeskryf word.

Prestasie

46. (1) Tensy die partye anders ooreengekom het, moet die leweransier die bestelling uitvoer binne 30 dae na die dag waarop die leweransier die bestelling ontvang het.

(2) Wanneer 'n leweransier versuim om die bestelling binne 30 dae of binne die ooreengekome tydperk uit te voer, kan die verbruiker die ooreenkoms met sewe dae geskrewe kennis beëindig.

(3) Indien 'n leweransier nie ingevolge die ooreenkoms uitvoering kan gee nie, op grond daarvan dat die bestelde goedere of dienste nie beskikbaar is nie, moet die leweransier die verbruiker onmiddellik van hierdie feit in kennis stel en enige betalings binne 30 dae na die datum van sodanige kennisgewing terugbetaal.

Toepaslikheid van buitelandse reg

47. Die beskerming wat in hierdie Hoofstuk aan verbruikers verleen word, is van toepassing ongeag die regstelsel wat op die betrokke ooreenkoms van toepassing is.

Nie-uitsluiting

48. Enige bepaling in 'n ooreenkoms wat die regte waarvoor in hierdie Hoofstuk voorsiening gemaak word, uitsluit, is ongeldig.

Klagtes aan Verbruikersakekomitee

49. 'n Verbruiker kan 'n klagte by die Verbruikersakekomitee indien ten opsigte van enige nie-nakoming van die bepalings van hierdie Hoofstuk deur 'n leweransier.

HOOFSTUK VIII

BESKERMING VAN PERSOONLIKE INLIGTING

Omvang van beskerming van persoonlike inligting

50. (1) Hierdie Hoofstuk is slegs van toepassing op persoonlike inligting wat deur middel van elektroniese transaksies verkry is.

(2) 'n Datakontroleur kan vrywilliglik die beginsels in artikel 51 vermeld, onderskryf deur sodanige feit in enige ooreenkoms met 'n datasubjek in te skryf.

(3) 'n Datakontroleur moet al die beginsels in artikel 51 vermeld, onderskryf en nie slegs dele daarvan nie.

(4) Die regte en verpligtinge van die partye met betrekking tot die skending van die beginsels in artikel 51 vermeld, word beheers deur die bedinge van enige ooreenkoms tussen hulle.

Beginsels vir elektroniese insameling van persoonlike inligting

51. (1) 'n Datakontroleur moet die uitdruklike geskrewe toestemming van die datasubjek hê vir die insameling, vergelyking, prosessering of openbaring van enige

for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.

(8) The data controller must delete or destroy all personal information which has become obsolete.

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

CHAPTER IX

PROTECTION OF CRITICAL DATABASES

Scope of critical database protection

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

Identification of critical data and critical databases

53. 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

54. (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

inligting oor daardie datasubjek, tensy hy of sy regtens toegelaat word of vereis word om dit te doen.

(2) 'n Datakontroleur mag nie persoonlike inligting oor 'n datasubjek wat nie nodig is vir die wettige doel waarvoor die persoonlike inligting vereis word elektronies versoek, insamel, vergelyk, prosesseer of berg nie.

(3) Die datakontroleur moet die spesifieke doel waarvoor enige persoonlike inligting versoek, ingesamel, vergelyk, geprosesseer of geberg word, skriftelik aan die datasubjek openbaar.

(4) Die datakontroleur mag nie sonder die uitdruklike geskrewe toestemming van die datasubjek persoonlike inligting vir 'n ander doel as die geopenbaarde doel gebruik nie, tensy hy of sy regtens toegelaat of vereis word om dit te doen.

(5) Die datakontroleur moet, solank die persoonlike inligting gebruik word en vir 'n tydperk van minstens een jaar daarna, 'n aantekening hou van die persoonlike inligting en die spesifieke doel waarvoor die persoonlike inligting ingesamel is.

(6) 'n Datakontroleur mag nie enige persoonlike inligting wat gehou word aan 'n derde party openbaar, tensy regtens vereis of toegelaat of spesifiek skriftelik deur die datasubjek daartoe gemagtig nie.

(7) Die datakontroleur moet, solank die persoonlike inligting gebruik word en vir 'n tydperk van minstens een jaar daarna, 'n rekord hou van enige derde party aan wie die persoonlike inligting geopenbaar is en van die datum waarop en die doel waarvoor dit geopenbaar is.

(8) Die datakontroleur moet alle persoonlike inligting wat verouderd geraak het, skrap of vernietig.

(9) 'n Party wat beskik oor persoonlike inligting kan daardie persoonlike inligting gebruik om profiele vir statistiese doeleindes saam te stel en kan vrylik handel dryf met sodanige profiele en statistiese data, solank die profiele of statistiese data nie deur 'n derde party gekoppel kan word aan enige spesifieke datasubjek nie.

HOOFSTUK IX

BESKERMING VAN KRITIEKE DATABASISSE

Bestek van beskerming van kritieke databasisse

52. Die bepalings van hierdie Hoofstuk is slegs van toepassing op 'n kritieke-databasisadministrateur en kritieke databasisse of dele daarvan.

Identifisering van kritieke data en kritieke databasisse

53. Die Minister kan by kennisgewing in die *Staatskoerant*—

(a) sekere klasse inligting wat van belang is vir die beskerming van die nasionale veiligheid van die Republiek of die ekonomiese en maatskaplike welsyn van sy burgers tot kritieke data vir die doeleindes van hierdie Hoofstuk verklaar; en

(b) prosedures instel wat by die identifisering van kritieke databasisse vir die doeleindes van hierdie Hoofstuk gevolg moet word.

Registrasie van kritieke databasisse

54. (1) Die Minister kan by kennisgewing in die *Staatskoerant*—

(a) vereistes bepaal vir die registrasie van kritieke databasisse by die Departement of die ander liggaam wat die Minister aanwys;

(b) prosedures bepaal wat vir registrasie gevolg moet word; en

(c) enige ander aangeleentheid met betrekking tot registrasie bepaal.

(2) By die toepassing van hierdie Hoofstuk beteken registrasie van 'n kritieke databasis die aanteken van die volgende inligting in 'n register wat deur die Departement of die ander liggaam wat die Minister aanwys, bygehou word:

(a) Die volle naam, adres en kontakbesonderhede van die administrateur van die kritieke databasis;

(b) die ligging van die kritieke databasis, met inbegrip van die ligging van konstituerende dele daarvan waar 'n kritieke databasis nie op 'n enkele plek geberg word nie;

(c) a general description of the categories or types of information stored in the critical database excluding the contents of such critical database.

Management of critical databases

55. (1) The Minister may prescribe minimum standards or prohibitions in respect of—

(a) the general management of critical databases;

(b) access to, transfer and control of critical databases;

(c) infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data;

(d) procedures and technological methods to be used in the storage or archiving of critical databases;

(e) disaster recovery plans in the event of loss of critical databases or parts thereof; and

(f) any other matter required for the adequate protection, management and control of critical databases.

(2) In respect of critical databases administered by public bodies, all regulations contemplated in subsection (1) must be made in consultation with all members of the Cabinet affected by the provisions of this Chapter: Provided that the Minister must not record information contemplated in section 54(2) if that information could reasonably compromise—

(a) the security of such databases; or

(b) the physical safety of a person in control of the critical database.

(3) This Chapter must not be construed so as to prejudice the right of a public body to perform any function authorised in terms of any other law.

Restrictions on disclosure of information

56. (1) Information contained in the register provided for in section 54 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) does not apply in respect of information which is disclosed—

(a) to a relevant authority which is investigating 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 for purposes of section 57;

(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 critical data or parts thereof.

Right of inspection

57. (1) The Director-General may, from time to time, cause audits to be performed at a critical database administrator to evaluate compliance with the provisions of this Chapter.

(2) The audit may be performed either by cyber inspectors or an independent auditor.

Non-compliance with Chapter

58. (1) Should the audit contemplated in section 57 reveal non-compliance by the critical database administrator with this Chapter, the Director-General must notify the critical database administrator thereof in writing, stating—

(a) the finding of the audit report;

(b) the action required to remedy the non-compliance; and

(c) the period within which the remedial action must be performed.

(c) 'n algemene beskrywing van die kategorieë of tipes inligting wat in die kritieke databasis geberg word, met uitsluiting van die inhoud van so 'n kritieke databasis.

Bestuur van kritieke databasisse

55. (1) Die Minister kan sekere minimum standaarde of verbiedinge voorskryf ten opsigte van—

(a) die algemene bestuur van kritieke databasisse;
(b) toegang tot, oordrag en beheer van kritieke databasisse;
(c) infrastrukturele of prosedurele reëls en vereistes om die integriteit en egtheid van kritieke data te verseker;
(d) prosedures en tegnologiese metodes wat gebruik moet word by die berging of bewaring van kritieke databasisse;
(e) rampherstelplanne in die geval van verlies van kritieke databasisse of dele daarvan; en
(f) enige ander aangeleentheid wat vereis word vir die voldoende beskerming, bestuur en beheer van kritieke databasisse.

(2) Ten opsigte van kritieke databasisse wat deur openbare liggame geadministreer word, moet alle regulasies wat in subartikel (1) beoog word, uitgevaardig word in oorleg met alle Kabinetslede wat deur die bepalings van hierdie Hoofstuk geraak word: Met dien verstande dat die Minister nie inligting in artikel 54(2) beoog moet aanteken nie indien daardie inligting redelikerwys—

(a) die sekerheid van sodanige databasisse kan aantas; of
(b) die fisiese veiligheid van 'n persoon in beheer van die kritieke databasis kan aantas.

(3) Hierdie Hoofstuk mag nie so uitgelê word dat dit die reg van 'n openbare liggaam aantas om enige werksaamheid te verrig wat ingevolge enige ander wetgewing gemagtig is nie.

Beperkings op openbaarmaking van inligting

56. (1) Inligting vervat in die register waarvoor in artikel 54 voorsiening gemaak word, mag nie aan enige persoon openbaargemaak word anders as aan werknemers van die Departement wat verantwoordelik is vir die hou van die register nie.

(2) Subartikel (1) is nie van toepassing nie ten opsigte van inligting wat openbaargemaak word—

(a) aan 'n toepaslike owerheid wat 'n kriminele oortreding ondersoek of vir die doeleindes van enige strafverrigtinge;
(b) aan regeringsinstansies wat verantwoordelik is vir veiligheid en sekuriteit in die Republiek na aanleiding van 'n amptelike versoek;
(c) aan 'n kuberinspekteur vir doeleindes van artikel 57;
(d) na aanleiding van artikels 11 en 30 van die Wet op Bevordering van Toegang tot Inligting, 2000; of
(e) vir doeleindes van enige siviele verrigtinge wat betrekking het op die kritieke data of dele daarvan.

Reg op inspeksie

57. (1) Die Direkteur-generaal kan, van tyd tot tyd, oudits laat uitvoer by 'n administrateur van 'n kritieke databasis om nakoming van die bepalings van hierdie Hoofstuk te evalueer.

(2) Die oudit kan deur kuberinspekteurs of 'n onafhanklike ouditeur uitgevoer word.

Nie-nakoming van Hoofstuk

58. (1) Indien die oudit wat in artikel 57 beoog word, nie-nakoming van hierdie Hoofstuk deur die administrateur van 'n kritieke databasis aantoon, moet die Direkteur-generaal die administrateur van die kritieke databasis skriftelik daarvan verwittig en—

(a) die bevindinge van die ouditverslag uiteensit;
(b) die handeling uiteensit wat vereis word om die nie-nakoming reg te stel; en
(c) die tyd uiteensit waarbinne die regstellingsaksie uitgevoer moet word.

(2) A critical database administrator that fails to take the remedial action within the period stated in the notice is guilty of an offence.

CHAPTER X

DOMAIN NAME AUTHORITY AND ADMINISTRATION

Part 1

Establishment and incorporation of .za domain name authority

Establishment of Authority

59. A juristic person to be known as the .za Domain Name Authority is hereby established for the purpose of assuming responsibility for the .za domain name space as from a date determined by the Minister by notice in the *Gazette* and by notifying all relevant authorities.

Incorporation of Authority

60. (1) The Minister must, within 12 months of the date of commencement of this Act, take all steps necessary for the incorporation of the Authority as a company contemplated in section 21(1) of the Companies Act, 1973 (Act No. 61 of 1973).

(2) All citizens and permanent residents of the Republic are eligible for membership of the Authority and must be registered as members upon application and on payment of a nominal fee to cover the cost of registration of membership and without having to comply with any formality.

(3) For the purpose of the incorporation of the Authority a person representing the Minister and the members of Namespace ZA as at the date of application for incorporation must be deemed to be members of the Authority.

Authority's memorandum and articles of association

61. (1) The memorandum of association and articles of association of the Authority must be consistent with this Chapter and, except where this Chapter provides to the contrary, also with the Companies Act, 1973 (Act No. 61 of 1973).

(2) Notwithstanding the Companies Act, 1973, an amendment to the memorandum of association or articles of association affecting any arrangement made by any provision of this Chapter, does not have any legal force and effect unless the Minister has consented in writing to such an amendment, which consent may not be withheld unreasonably.

(3) No fee is payable in terms of the Companies Act, 1973, in respect of the reservation of the name of the company, the registration of the said memorandum and articles and the issue of the certificate to commence business.

(4) The memorandum and articles of association of the Authority must, amongst others, provide for—

(a) the rules for the convening and conducting of meetings of the Board, including the quorum required for and the minutes to be kept of those meetings;

(b) the manner in which decisions are to be made;

(c) the establishment of any division of the Authority to perform specialised functions;

(d) the establishment and functioning of committees, including a management committee;

(e) the co-opting by the Board or a committee of any person to assist the Authority or committee in the consideration of any particular matter;

(f) the preparation by the Board of an annual business plan in terms of which the activities of the Authority are planned annually;

(g) the banking and investment of funds by the Board;

(h) provisions to regulate the manner in which, and procedures whereby, expertise from any person is obtained in order to further the objects of the Authority;

(2) Die administrateur van 'n kritieke databasis wat nalaat om die regstellingsaksie uit te voer binne die tydperk wat in die kennisgewing aangegee word, is skuldig aan 'n misdryf.

HOOFSTUK X

DOMEINNAAMOWERHEID EN ADMINISTRASIE

Deel 1

Instelling en inlywing van .za-Domeinnaamowerheid

Instelling van Owerheid

59. 'n Regspersoon word hierby ingestel wat bekend moet staan as die .za-Domeinnaamowerheid, met die doel om verantwoordelikheid te aanvaar vir die .za-domeinnaamruimte vanaf 'n datum bepaal deur die Minister by kennisgewing in die *Staatskoerant* en by kennisgewing aan alle relevante owerhede.

Inlywing van Owerheid

60. (1) Die Minister moet 12 maande vanaf die datum van inwerkingtreding van hierdie Wet, alle stappe doen wat nodig is vir die inlywing van die Owerheid as 'n maatskappy beoog in artikel 21(1) van die Maatskappywet, 1973 (Wet No. 61 van 1973).

(2) Alle burgers en permanente inwoners van die Republiek is benoembaar vir lidmaatskap van die Owerheid en moet op aansoek geregistreer word as lede, teen betaling van 'n nominale bedrag om die koste van registrasie van lidmaatskap te dek, en sonder dat aan enige formaliteit voldoen hoef te word.

(3) Met die oog op die inlywing van die Owerheid moet 'n persoon wat die Minister verteenwoordig en die lede van Namespace ZA soos op die datum van die aansoek vir inlywing, geag word lede van die Owerheid te wees.

Owerheid se akte van oprigting en statute

61. (1) Die akte van oprigting en statute van die Owerheid moet met hierdie Hoofstuk en, behalwe waar hierdie Hoofstuk anders bepaal, ook met die Maatskappywet, 1973 (Wet No. 61 van 1973), bestaanbaar wees.

(2) Ondanks die Maatskappywet, 1973, het 'n wysiging van die akte van oprigting en statute wat 'n uitwerking het op enige reëling deur enige bepaling van hierdie Hoofstuk getref, geen regskrag en regswerking nie tensy die Minister skriftelik tot sodanige wysiging ingestem het, welke instemming nie onredelik weerhou mag word nie.

(3) Geen geld is betaalbaar ingevolge die Maatskappywet, 1973, ten opsigte van die reservering van die naam van die maatskappy, die registrasie van die vermelde akte van oprigting en statute en die uitreiking van die sertifikaat om met besigheid te begin nie.

(4) Die akte van oprigting en statute van die Owerheid moet, onder andere, voorsiening maak vir—

(a) die reëls vir die belê en hou van vergaderings van die Raad, met inbegrip van die kworum vereis vir en die notule wat gehou moet word van daardie vergaderings;

(b) die wyse waarop besluite geneem moet word;

(c) die instelling van enige afdeling van die Owerheid om gespesialiseerde werksaamhede te verrig;

(d) die instelling en werking van komitees, met inbegrip van 'n bestuurskomitee;

(e) die koöptering deur die Raad of 'n komitee van enige persoon om die Owerheid of komitee met die oorweging van enige besondere aangeleentheid by te staan;

(f) die voorbereiding deur die Raad van 'n jaarlikse besigheidsplan ingevolge waarvan die bedrywighede van die Owerheid jaarliks beplan word;

(g) die bank en belegging van fondse deur die Raad;

(h) bepalings ter reëling van die wyse waarop, en die prosedures waarvolgens, kundigheid van enige persoon verkry kan word om die oogmerke van die Owerheid te bevorder;

(i) the determination through arbitration of any dispute concerning the interpretation of the memorandum and articles of association of the Authority;

(j) the delegation of powers and assignment of duties to directors, committees and employees: Provided that the Board may—

(i) not be divested of any power or duty by virtue of the delegation or assignment; and

(ii) vary or set aside any decision made under any delegation or in terms of any assignment;

(k) the procedures and criteria for the establishment and disestablishment of second level domains and for delegations to such domains;

(l) appeal mechanisms;

(m) the tenure of directors;

(n) the circumstances under and the manner in which a directorship is terminated;

(o) criteria for the disqualification of directors;

(p) the method of determining the allowances to be paid to directors for attending meetings; and

(q) the powers and duties of directors.

Part 2

Governance and staffing of Authority

Board of directors of Authority

62. (1) The Authority is managed and controlled by a Board of Directors consisting of nine directors, one of whom is the chairperson.

(2) The process of appointment is the following:

(a) The Minister must appoint an independent selection panel consisting of five persons, who command public respect for their fair-mindedness, wisdom and understanding of issues concerning the Internet, culture, language, academia and business, the names of whom must be placed in a notice in the *Gazette*;

(b) the Minister must invite nominations for members of the Board from the public through newspapers which have general circulation throughout the Republic, on-line news services, radio and by notice in the *Gazette*;

(c) nominations must be made to the panel established in terms of paragraph *(a)*;

(d) the panel must recommend to the Minister names of nine persons to be appointed to the Board taking into account the sectors of stakeholders listed in subsection (3)*(b)*;

(e) if the Minister is not satisfied that the recommendations of the panel comply with subsection (3) the Minister may request the panel to review its recommendations and make new ones;

(f) the Minister must appoint the members of the Board, and publish the names of those appointed in the *Gazette*;

(g) the Minister must appoint the Chairperson of the Board from among the names recommended by the panel.

(3) *(a)* The Board, when viewed collectively, must be broadly representative of the demographics of the country, including having regard to gender and disability.

(b) Sectors of stakeholders contemplated in subsection (2)*(d)* are—

(i) The existing Domain Name community;

(ii) Academic and legal sectors;

(iii) Science, technology and engineering sectors;

(iv) Labour;

(v) Business and the private sector;

(vi) Culture and language;

(vii) Public sector;

(viii) Internet user community.

(4) Directors must be persons who are committed to fairness, openness and accountability and to the objects of this Act.

(i) die beslegting deur arbitrasie van enige geskil aangaande die uitleg van die akte van oprigting en statute van die Owerheid;

(j) die delegering van bevoegdhede en opdra van pligte aan direkteure, komitees en werknemers: Met dien verstande dat die Raad—

(i) nie van enige bevoegdheid of plig uit hoofde van die delegasie of opdrag ontneem mag word nie; en

(ii) enige besluit geneem kragtens enige delegering of ingevolge enige opdrag kan verander of ter syde kan stel;

(k) die prosedures en kriteria vir die oprigting en opsegging van tweedevlakdomeine aan sulke domeine;

(l) appèlmeganismes;

(m) die ampstermyn van direkteure;

(n) die omstandighede waaronder en die wyses waarop 'n direkteurskap beëindig word;

(o) kriteria vir die diskwalifikasie van direkteure;

(p) die wyse waarop toelaes vasgestel word wat aan direkteure betaal moet word vir bywoon van vergaderings; en

(q) die bevoegdhede en pligte van direkteure.

Deel 2

Bestuur en personeelvoorsiening van Owerheid

Raad van direkteure van Owerheid

62. (1) Die Owerheid word bestuur en beheer deur 'n Raad van direkteure wat bestaan uit nege direkteure, van wie een die voorsitter is.

(2) Die aanstellingsproses is soos volg:

(a) Die Minister moet 'n onafhanklike kiespaneel aanstel wat bestaan uit vyf persone wat openbare respek afdwing vir hulle regverdigheidsin, wysheid en begrip van kwessies rakende die Internet, kultuur, taal, die akademie en die sakewêreld, wie se name in 'n kennisgewing in die *Staatskoerant* gepubliseer moet word;

(b) die Minister moet 'n uitnodiging rig aan die publiek vir nominasies vir lede van die Raad deur middel van koerante wat algemene sirkulasie deur die hele Republiek het, gekoppelde nuusdienste, radio en by kennisgewing in die *Staatskoerant;*

(c) nominasies moet gedoen word aan die paneel wat ingevolge paragraaf *(a)* saamgestel is;

(d) die paneel moet by die Minister aanbeveel die name van nege persone om in die Raad aangestel te word met inagnememing van die sektore van belanghebbendes wat in subartikel 3*(b)* vermeld word;

(e) indien die Minister nie oortuig is dat die aanbeveling van die paneel aan subartikel (3) voldoen nie, kan die Minister die paneel vra om die aanbeveling te hersien en nuwe aanbevelings te maak;

(f) die Minister moet die lede van die Raad aanstel, en die name van diegene wat aangestel is in die *Staatskoerant* publiseer;

(g) die Minister moet die Voorsitter van die Raad aanstel vanuit die name wat deur die paneel aanbeveel is.

(3) *(a)* Die Raad, in sy geheel gesien, moet breedweg verteenwoordigend wees van die demografie van die land, ook met verwysing na geslag en gestremdheid.

(b) Sektore van belanghebbendes soos in subartikel 2*(d)* bedoel, is—

(i) Die bestaande Domeinnaamgemeenskap;

(ii) Akademiese en regsektore;

(iii) Wetenskap-, tegnologie- en ingenieursektore;

(iv) Arbeid;

(v) Sake en die privaatsektor;

(vi) Kultuur en taal;

(vii) Openbare sektor;

(viii) Internetgebruikersgemeenskap.

(4) Direkteure moet persone wees wat verbind is tot regverdigheid, openheid en verantwoordbaarheid en aan die oogmerke van hierdie Wet.

(5) All directors serve in a part-time and non-executive capacity.

(6) Any vacancy on the Board must be filled in accordance with subsections (2) and (3).

Staff of Authority

63. (1) The chief executive officer of the Authority appointed by the Board must perform any work incidental to the functions of the Authority.

(2) The chief executive officer must be assisted by staff appointed by the Board.

(3) The Board must determine the conditions of service, remuneration and service benefits of the chief executive officer and the staff.

(4) If the chief executive officer is for any reason unable to perform his or her functions, the Board may designate a person in the service of the Authority to act as the acting chief executive officer until the chief executive officer is able to resume office.

Part 3

Functions of Authority

Licensing of registrars and registries

64. (1) No person may update a repository or administer a second level domain unless such person is licensed to do so by the Authority.

(2) An application to be licensed as a registrar or registry must be made in the prescribed manner and subject to the prescribed fees.

(3) The Authority must apply the prescribed conditions and criteria when evaluating an application referred to in subsection (2).

Functions of Authority

65. (1) The Authority must—

(a) administer and manage the .za domain name space;

(b) comply with international best practice in the administration of the .za domain name space;

(c) license and regulate registries;

(d) license and regulate registrars for the respective registries; and

(e) publish guidelines on—

(i) the general administration and management of the .za domain name space;

(ii) the requirements and procedures for domain name registration; and

(iii) the maintenance of and public access to a repository,

with due regard to the policy directives which the Minister may make from time to time by notice in the *Gazette*.

(2) The Authority must enhance public awareness on the economic and commercial benefits of domain name registration.

(3) The Authority—

(a) may conduct such investigations as it may consider necessary;

(b) must conduct research into and keep abreast of developments in the Republic and elsewhere on the domain name system;

(c) must continually survey and evaluate the extent to which the .za domain name space meets the needs of the citizens of the Republic; and

(d) may, from time to time, issue information on the registration of domain names in the Republic.

(4) The Authority may, and must when so requested by the Minister, make recommendations to the Minister in relation to policy on any matter relating to the .za domain name space.

(5) The Authority must continually evaluate the effectiveness of this Act and things done in terms thereof towards the management of the .za domain name space.

(6) The Authority may—

(a) liaise, consult and co-operate with any person or other authority; and

(b) appoint experts and other consultants on such conditions as the Authority may determine.

(5) Alle direkteure dien in 'n deeltydse en nie-uitvoerende hoedanigheid.

(6) Enige vakature in die Raad moet gevul word ingevolge subartikels (2) en (3).

Personeel van Owerheid

63. (1) Die hoof- uitvoerende beampte van die Owerheid wat deur die Raad aangestel word, moet alle werk verbonde aan die werksaamhede van die Owerheid uitvoer.

(2) Die hoof- uitvoerende beampte moet bygestaan word deur personeel wat deur die Raad aangestel word.

(3) Die Raad moet die diensvoorwaardes, vergoeding en diensvoordele van die hoof-uitvoerende beampte en die personeel bepaal.

(4) Indien die hoof- uitvoerende beampte om enige rede nie in staat is om sy of haar werksaamhede te verrig nie, kan die Raad 'n persoon in diens van die Owerheid aanwys om as waarnemende hoof- uitvoerende beampte op te tree totdat die hoof- uitvoerende beampte in staat is om diens te hervat.

Deel 3

Werksaamhede van Owerheid

Lisensiëring van registrateurs en registrasiekantore

64. (1) Geen persoon mag 'n bewaarplek op datum bring of 'n tweedevlakdomein administreer tensy sodanige persoon deur die Owerheid gelisensieër is om dit te doen nie.

(2) 'n Aansoek om as 'n registrateur of registrasiekantoor gelisensieër te word, moet op die voorgeskrewe wyse en behoudens die voorgeskrewe gelde gedoen word.

(3) Die Owerheid moet die voorgeskrewe voorwaardes en kriteria toepas wanneer 'n aansoek in subartikel (2) bedoel, geëvalueer word.

Werksaamhede van Owerheid

65. (1) Die Owerheid moet—

(a) die .za-domeinnaamruimte administreer en bestuur;

(b) voldoen aan die internasionale beste praktyk in die administrasie van die .za-domeinnaamruimte;

(c) registrasiekantore lisensieer en reël;

(d) registrateurs vir die onderskeie registrasiekantore lisensieer en reël; en

(e) riglyne publiseer oor—

(i) die algemene administrasie en bestuur van die .za-domeinnaamruimte;

(ii) die vereistes en prosedures vir domeinnaamregistrasie; en

(iii) die onderhou van en openbare toegang tot 'n bewaarplek,

met behoorlike inagneming van die beleidslasgewings wat die Minister van tyd tot tyd by kennisgewing in die *Staatskoerant* kan uitvaardig.

(2) Die Owerheid moet openbare bewustheid aangaande die ekonomiese en kommersiële voordele van domeinnaamregistrasie bevorder.

(3) Die Owerheid—

(a) kan dié ondersoeke loods wat hy nodig ag;

(b) moet navorsing doen oor en op die hoogte bly van ontwikkelings in die Republiek en elders oor die domeinnaamstelsel;

(c) moet voortdurend die mate waarin die .za-domeinnaamruimte voldoen aan die behoeftes van die burgers van die Republiek besigtig en evalueer; en

(d) kan, van tyd tot tyd, inligting uitreik oor die registrasie van domeinname in die Republiek.

(4) Die Owerheid kan, en moet wanneer deur die Minister daartoe versoek, aanbevelings aan die Minister doen met betrekking tot beleid aangaande enige aangeleentheid wat op die .za-domeinnaamruimte betrekking het.

(5) Die Owerheid moet voortdurend die doeltreffendheid van hierdie Wet evalueer en dinge wat ingevolge daarvan insake die bestuur van die .za-domeinnaamruimte gedoen word.

(6) Die Owerheid kan—

(a) met enige persoon of ander owerheid skakel, oorleg pleeg en saamwerk; en

(b) deskundiges en ander konsultante aanstel op die voorwaardes as wat die Owerheid bepaal.

(7) The Authority must respect and uphold the vested rights and interests of parties that were actively involved in the management and administration of the .za domain name space at the date of its establishment: Provided that—

(a) such parties must be granted a period of six months during which they may continue to operate in respect of their existing delegated sub-domains; and

(b) after the expiry of the six-month period, such parties must duly apply to be licensed registrars and registries as provided for in this Part.

Part 4

Finances and reporting

Finances of Authority

66. (1) All money received by the Authority must be deposited in a banking account in the name of the Authority with a bank established under the Banks Act, 1990 (Act No. 94 of 1990), or a mutual bank established under the Mutual Banks Act, 1993 (Act No. 124 of 1993).

(2) The chief executive officer is the accounting officer of the Authority and must ensure that—

(a) proper record of all the financial transactions, assets and liabilities of the Authority are kept; and

(b) as soon as possible, but not later than three months after the end of a financial year, accounts reflecting the income and expenditure of the Authority and a balance sheet of the assets and liabilities of the Authority as at the end of that financial year are prepared and submitted to the Board and Minister.

(3) The Authority is funded from—

(a) the capital invested in or lent to the Authority;

(b) money appropriated by Parliament for that purpose;

(c) income derived from the sale or other commercial exploitation of its licenses, approvals, products, technology, services or expertise in terms of this Act;

(d) loans raised by the Authority;

(e) the proceeds of any sale of assets;

(f) income or interest earned on the Authority's cash balances or on money invested by it; and

(g) money received by way of grant, contribution, donation or inheritance from any source inside or outside the Republic.

(4) The funds of the Authority must be utilised to meet the expenditure incurred by the Authority in connection with its functioning, business and operations in terms of this Act.

(5) *(a)* The money may be so utilised only as provided for in a statement of the Authority's estimated income and expenditure, that has been approved by the Minister.

(b) Money received by way of grant, contribution, donation or inheritance in terms of subsection (3)*(g)*, must be utilised in accordance with any conditions imposed by the grantor, contributor, donor or testator concerned.

(6) *(a)* The Board must in each financial year, at a time determined by the Minister, submit to the Minister for approval a statement of the Authority's estimated income and expenditure for the next financial year.

(b) The Board may at any time during the course of a financial year, submit a supplementary statement of estimated income and expenditure of the Authority for that financial year, to the Minister for approval.

(c) The Minister may grant the approval of the statement referred to in paragraph *(a)*, with the agreement of the Minister of Finance.

(d) The Authority may not incur any expenditure in excess of the total amount approved under paragraph *(c)*.

(7) The Board may establish a reserve fund for any purpose that is connected with the Authority's functions under this Act and has been approved by the Minster, and may allocate to the reserve fund the money that may be made available for the purposes in the

(7) Die Owerheid moet die gevestigde regte en belange respekteer en ondersteun van partye wat aktief met die bestuur en administrasie van die .za-domeinnaamruimte gemoeid was ten tyde van sy instelling: Met dien verstande dat—

(a) sodanige partye 'n tydperk van ses maande verleen moet word waartydens hulle kan voortgaan om ten opsigte van hul bestaande gedelegeerde subdomeine op te tree; en

(b) na die verstryking van die tydperk van ses maande, sodanige partye behoorlik aansoek moet doen om gelisensieerde registrateurs en registrasiekantore te wees soos waarvoor in hierdie Deel voorsiening gemaak word.

Deel 4

Finansies en verslagdoening

Finansies van Owerheid

66. (1) Alle gelde wat deur die Owerheid ontvang word, moet gedeponeer word in 'n bankrekening in die naam van die Owerheid by 'n bank wat kragtens die Bankwet, 1990 (Wet No. 94 van 1990), of by 'n onderlinge bank wat kragtens die Wet op Onderlinge Banke, 1993 (Wet No. 124 van 1993), opgerig is.

(2) Die hoof- uitvoerende beampte is die rekenpligtige beampte van die Owerheid, en moet verseker dat—

(a) behoorlik rekord gehou word van al die finansiële transaksies, bates en laste van die Owerheid; en

(b) so gou as moontlik, maar nie later nie as drie maande na die einde van 'n boekjaar, rekeningstate wat die inkomste en uitgawes van die Owerheid weergee en 'n balansstaat van die bates en laste van die Owerheid soos aan die einde van die boekjaar, opgestel word en aan die Raad en Minister voorgelê word.

(3) Die Owerheid word gefinansier vanuit—

(a) die kapitaal wat in die Owerheid belê of daaraan geleen is;

(b) geld wat deur die Parlement vir daardie doel bewillig is;

(c) inkomste verkry uit die verkoop of ander kommersiële benutting van sy lisensies, goedkeurings, produkte, tegnologie, dienste of kundigheid ingevolge hierdie Wet;

(d) lenings wat deur die Owerheid aangegaan is;

(e) die opbrengste van enige verkoop van bates;

(f) inkomste of rente verdien op die Owerheid se kontantbalanse, of op geld daardeur belê; en

(g) geld wat ontvang is by wyse van toewysing, bydrae, donasie of erfenis van enige bron, binne of buite die Republiek.

(4) Die fondse van die Owerheid moet gebruik word om uitgawes te dek wat deur die Owerheid aangegaan is in verband met sy funksionering, besigheid en bedrywighede ingevolg hierdie Wet.

(5) *(a)* Die gelde mag so gebruik word slegs soos daarvoor voorsiening gemaak is in 'n staat van die Owerheid se geraamde inkomste en uitgawes wat deur die Minister goedgekeur is.

(b) Geld wat by wyse van toewysing, bydrae, donasie of erfenis ingevolge subartikel (3)*(g)* ontvang is, moet aangewend word ooreenkomstig enige voorwaardes wat deur die betrokke toekenner, bydraer, donateur of erflater opgelê is.

(6) *(a)* Die Raad moet in elke boekjaar, op 'n tyd deur die Minister vasgestel, aan die Minister vir goedkeuring 'n staat van die Owerheid se geraamde inkomste en uitgawes vir die volgende boekjaar voorlê.

(b) Die Raad kan te eniger tyd in die loop van 'n boekjaar, 'n bykomende staat van geraamde inkomste en uitgawes van die Owerheid vir daardie boekjaar voor die Minister vir goedkeuring voorlê.

(c) Die Minister kan goedkeuring verleen aan die staat in paragraaf *(a)* bedoel, met die goedkeuring van die Minister van Finansies.

(d) Die Owerheid mag nie enige uitgawes aangaan wat die totale bedrag wat kragtens paragraaf *(c)* goedgekeur is, oorskry nie.

(7) Die Raad kan 'n reserwefonds stig vir enige doel wat met die Owerheid se werksaamhede kragtens hierdie Wet verband hou en wat deur die Minister goedgekeur is, en kan aan die reserwefonds toewys die geld wat vir die doeleindes beskikbaar gestel

statement of estimated income and expenditure or supplementary statement contemplated in subsection (6).

(8) To the extent that the Authority is provided with start-up capital by the State, the Authority may, at the election of the Minister of Finance, be made subject to the Public Finance Management Act, (Act No. 1 of 1999), until such time as the Authority, to the satisfaction of the Minister of Finance, becomes self-sustaining through the alternative sources of revenue provided for in subsection (3).

Reports

67. As soon as practicable after the end of every financial year, the Board must submit a report on its activities during that year to the Minister who must table that report in Parliament.

Part 5

Regulations

Regulations regarding Authority

68. The Authority may, with the approval of the Minister, make regulations regarding—

(a) the requirements which registries and registrars must meet in order to be licensed, including objective standards relating to operational accuracy, stability, robustness and efficiency;

(b) the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries with due regard to the express recognition of the right of groups and members of groups within the Republic to identify with, use or communicate cultural, linguistic, geographical, indigenous or any other expressions of heritage including any visual or audible elements or attributes thereof;

(c) pricing policy;

(d) provisions for the restoration of a domain name registration and penalties for late payments;

(e) the terms of the domain name registration agreement which registries and registrars must adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution;

(f) processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of actual or prospective registrants, registries or registrars, protocols or products;

(g) requirements to ensure that each domain name contains an administrative and technical contact;

(h) the creation of new sub-domains;

(i) procedures for ensuring monitoring of compliance with the provisions of this Act and the regulations provided for in this Chapter, including regular .za domain name space technical audits;

(j) such other matters relating to the .za domain name space as it may be necessary to prescribe to achieve the objectives of this Chapter; and

(k) policy to be applied by the Authority.

word in die staat van geraamde inkomste en uitgawes of bykomende staat in subartikel (6) beoog.

(8) In die mate wat die Owerheid van wegspringkapitaal deur die Staat voorsien word, kan die Owerheid, ten keuse van die Minister van Finansies, onderworpe gestel word aan die Wet op Openbare Finansiële Bestuur, (Wet No. 1 van 1999), tot tyd en wyl die Owerheid, na die bevrediging van die Minister van Finansies, selfonderhoudend word deur die alternatiewe inkomstebronne waarvoor daar in subartikel (3) voorsiening gemaak word.

Verslae

67. So gou doenlik na die einde van elke boekjaar, moet die Raad 'n verslag oor sy bedrywighede gedurende daardie jaar voorlê aan die Minister wat dan daardie verslag in die Parlement ter tafel moet lê.

Deel 5

Regulasies

Regulasies aangaande Owerheid

68. (1) Die Owerheid kan, met die goedkeuring van die Minister, regulasies uitvaardig aangaande—

(a) die vereistes waaraan registrasiekantore en registrateurs moet voldoen ten einde gelisensieer te word, met inbegrip van objektiewe standaarde met betrekking tot operasionele akkuraatheid, stabiliteit, kragdadigheid en effektiwiteit;

(b) die omstandighede waaronder en die wyse waarop registrasies opgedra, geregistreer, hernu, geweier of herroep kan word deur die registrasiekantore, met die behoorlike inagneming van die uitdruklike erkenning van die reg van groepe en lede van groepe binne die Republiek om hulle te identifiseer met kultuur-, taal-, geografiese, inheemse of ander uitdrukkings van erfenis, met inbegrip van enige sigbare of hoorbare elemente of kenmerke daarvan, of om dit te gebruik of te kommunikeer;

(c) prysvasstellingsbeleid;

(d) bepalings vir die herstel van 'n domeinnaamregistrasie en strawwe vir laat betalings;

(e) die bedinge van die ooreenkoms vir die domeinnaamregistrasie wat registrasiekantore en registrateurs moet aanneem en gebruik by die registrasie van domeinname, met inbegrip van kwessies ten opsigte van privaatheid, verbruikersbeskerming en alternatiewe geskilbeslegting;

(f) prosesse en prosedures om onregverdige en nie-mededingende praktyke te vermy, met inbegrip van vooroordeel teenoor, of voorkeurbehandeling van, werklike of voornemende geregistreerdes, registrasiekantore of registrateurs, protokolle of produkte;

(g) vereistes om te verseker dat elke domeinnaam 'n administratiewe en tegniese kontak bevat;

(h) die skepping van nuwe subdomeine;

(i) prosedures om die monitering van nakoming van die bepalings van hierdie Wet en die regulasies waarvoor in hierdie Hoofstuk voorsiening gemaak word, met inbegrip van gereelde tegniese oudits van die .za-domeinnaamruimte, te verseker;

(j) sodanige ander aangeleenthede met betrekking tot die .za-domeinnaamruimte wat nodig is om voor te skryf om die oogmerke van hierdie Hoofstuk te bereik; en

(k) beleid wat deur die Owerheid toegepas moet word.

Part 6

Alternative dispute resolution

Alternative dispute resolution

69. (1) The Minister, in consultation with the Minister of Trade and Industry, must make regulations for an alternative mechanism for the resolution of disputes in respect of the .za domain name space.

(2) The regulations must be made with due regard to existing international precedent.

(3) The regulations may prescribe—

(a) procedures for the resolution of certain types of disputes determined in the regulations and which relate to a domain name registration;

(b) the role which the Authority must fulfil in administering the dispute resolution procedure;

(c) the appointment, role and function of dispute resolution adjudicators;

(d) the procedure and rules which must be followed in adjudicating disputes;

(e) unlawful actions or activities in respect of domain names, distinguishing between criminal and civil liability;

(f) measures to prevent unlawful actions or activities with respect to domain names;

(g) the manner, costs of and time within which a determination must be made;

(h) the implementation of determinations made in terms of the dispute resolution procedure;

(i) the limitation of liability of registrars and registries for implementing a determination; and

(j) the enforcement and publication of determinations.

CHAPTER XI

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

Definition

70. In this Chapter, "service provider" means any person providing information system services.

Recognition of representative body

71. (1) The Minister may, on application by an industry representative body for service providers by notice in the *Gazette*, recognise such body for purposes of section 72.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that—

(a) its members are subject to a code of conduct;

(b) membership is subject to adequate criteria;

(c) the code of conduct requires continued adherence to adequate standards of conduct; and

(d) the representative body is capable of monitoring and enforcing its code of conduct adequately.

Conditions for eligibility

72. The limitations on liability established by this Chapter apply to a service provider only if—

(a) the service provider is a member of the representative body referred to in section 71; and

Deel 6

Alternatiewe geskilbeslegting

Alternatiewe geskilbeslegting

69. (1) Die Minister, in oorleg met die Minister van Handel en Nywerheid, moet regulasies uitvaardig vir 'n alternatiewe meganisme vir die beslegting van geskille ten opsigte van die .za-domeinnaamruimte.

(2) Die regulasies moet uitgevaardig word met behoorlike inagneming van internasionale presedent.

(3) Die regulasies kan—

(a) geskilbeslegtingsprosedures voorskryf in die geval van sekere tipes geskille wat in die regulasies bepaal word en wat op 'n domeinnaamregistrasie betrekking het;

(b) die rol voorskryf wat die Owerheid moet vervul by die administrasie van die geskilbeslegtingsprosedure;

(c) die aanstelling, rol en werksaamheid van geskilbeslegtingsberegters voorskryf;

(d) die prosedure en reëls wat by die beregting van geskille gevolg moet word, voorskryf;

(e) onwettige optrede of handelinge ten opsigte van domeinname voorskryf, terwyl tussen strafregtelike en siviele aanspreeklikheid onderskei word;

(f) maatreëls voorskryf om onwettige optrede of handelinge ten opsigte van domeinname te verhinder;

(g) die wyse waarop koste van en tyd waarbinne 'n vasstelling gemaak moet word, voorskryf;

(h) die implementering voorskryf van vasstellings wat ingevolge die geskilbeslegtingsprosedures gemaak is;

(i) die beperking van aanspreeklikheid van registrateurs en registrasiekantore vir die implementering van 'n vasstelling voorskryf; en

(j) die afdwinging en publikasie van vasstellings voorskryf.

HOOFSTUK XI

BEPERKING VAN AANSPREEKLIKHEID VAN DIENSVERSKAFFERS

Woordomskrywing

70. In hierdie Hoofstuk beteken "diensverskaffer" enige persoon wat inligtingstelseldienste verskaf.

Erkenning van verteenwoordigende liggaam

71. (1) Die Minister kan, op aansoek deur 'n bedryfsverteenwoordigende liggaam vir diensverskaffers, sodanige liggaam by kennisgewing in die *Staatskoerant* erken vir die doeleindes van artikel 72.

(2) Die Minister kan slegs 'n verteenwoordigende liggaam in subartikel (1) bedoel, erken indien die Minister tevrede is dat—

(a) sy lede aan 'n gedragskode onderworpe is;

(b) lidmaatskap aan voldoende kriteria onderworpe is;

(c) die gedragskode voortdurende ondersteuning van voldoende standaarde van gedrag vereis; en

(d) die verteenwoordigende liggaam in staat is om sy gedragskode voldoende te moniteer en af te dwing.

Voorwaardes van toepaslikheid

72. Die beperkings op aanspreeklikheid by hierdie Hoofstuk ingestel, is slegs op 'n diensverskaffer van toepassing indien—

(a) die diensverskaffer 'n lid is van die verteenwoordigende liggaam bedoel in artikel 71; en

(*b*) the service provider has adopted and implemented the official code of conduct of that representative body.

Mere conduit

73. (1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider—

(*a*) does not initiate the transmission;

(*b*) does not select the addressee;

(*c*) performs the functions in an automatic, technical manner without selection of the data; and

(*d*) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—

(*a*) for the sole purpose of carrying out the transmission in the information system;

(*b*) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and

(*c*) for a period no longer than is reasonably necessary for the transmission.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Caching

74. (1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—

(*a*) does not modify the data;

(*b*) complies with conditions on access to the data;

(*c*) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;

(*d*) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the data; and

(*e*) removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 77.

(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Hosting

75. (1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider—

(*a*) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or

(*b*) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(*c*) upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

(b) die diensverskaffer die amptelike gedragskode van daardie verteenwoordigende liggaam aangeneem en geïmplementeer het.

Blote geleibuis

73. (1) 'n Diensverskaffer is nie aanspreeklik vir verskaffing van toegangsverbindings tot, of vir die bedryf van fasiliteite vir inligtingstelsels, of versending, roetering of berging van databoodskappe via 'n inligtingstelsel onder sy of haar beheer nie, mits die diensverskaffer—

(a) nie die versending begin nie;

(b) nie die geadresseerde kies nie;

(c) die werksaamhede op 'n outomatiese, tegniese wyse verrig sonder selektering van die data; en

(d) nie die data vervat in die versending verander nie.

(2) Die handelinge van versending, roetering en van verskaffing van toegang bedoel in subartikel (1) sluit in die outomatiese, tussentydse en kortstondige berging van die versende inligting, vir sover dit plaasvind—

(a) vir die uitsluitlike doel om die versending in die inligtingstelsel uit te voer;

(b) op 'n wyse wat dit gewoonweg ontoeganklik maak vir enigeen anders as verwagte ontvangers; en

(c) vir 'n tydperk wat nie langer is as wat redelikerwys vir die versending nodig is nie.

(3) Ondanks hierdie artikel kan 'n bevoegde hof 'n diensverskaffer beveel om onwettige bedrywigheid ingevolge enige ander wet te staak of te verhinder.

Berging in kasgeheue

74. (1)'n Diensverskaffer wat data versend wat deur 'n ontvanger van die diens verskaf word via 'n inligtingstelsel onder sy of haar beheer is nie aanspreeklik nie vir die outomatiese, tussentydse en tydelike berging van daardie data, waar die doel van die berging van sodanige data is om die verdere versending van die data na ander ontvangers van die diens op hul versoek meer effektief te maak, solank die diensverskaffer—

(a) nie die data verander nie;

(b) voldoen aan die voorwaardes van toegang tot die data;

(c) voldoen aan reëls met betrekking tot die opdatering van die data, uiteengesit op 'n wyse wat wyd erken en gebruik word deur die bedryf;

(d) nie inmeng met die wettige gebruik van tegnologie, wat wyd erken en gebruik word deur die bedryf, om inligting oor die gebruik van die data te verkry nie; en

(e) toegang tot data wat geberg is, verwyder of ongeskik maak by ontvangs van 'n afhaalkennisgewing bedoel in artikel 77.

(2) Ondanks hierdie artikel kan 'n bevoegde hof 'n diensverskaffer gebied om onwettige bedrywigheid ingevolge enige ander wet te staak of te verhinder.

Gasheer wees

75. (1) 'n Diensverskaffer wat 'n diens verskaf wat bestaan uit die berging van data wat deur 'n ontvanger van die diens verskaf word, is nie aanspreeklik vir skade wat ontstaan weens data wat op die versoek van die ontvanger van die diens geberg word nie, solank die diensverskaffer—

(a) nie werklike kennis het dat die databoodskap of 'n bedrywigheid in verband met die databoodskap die regte van 'n derde party skend nie; of

(b) nie bewus is van feite of omstandighede waaruit die skendende bedrywigheid of die skendende aard van die databoodskap blyk nie; en

(c) by ontvangs van 'n afhaalkennisgewing bedoel in artikel 77, spoedig optree om toegang tot die data te verwyder of ongeskik te maak.

(2) Die beperkings op aanspreeklikheid by hierdie artikel ingestel, is nie van toepassing op 'n diensverskaffer nie tensy hy of sy 'n agent aangestel het om kennisgewings van skendings te ontvang en deur sy of haar dienste, ook op sy of haar webwerwe op plekke wat vir die publiek toeganklik is, die naam, adres, telefoonnommer en e-posadres van die agent voorsien het.

(3) Ondanks hierdie artikel kan 'n bevoegde hof 'n diensverskaffer beveel om onwettige bedrywigheid ingevolge enige ander wet te staak of verhinder.

(4) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

Information location tools

76. A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider—

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

Take-down notification

77. (1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include—

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith;

(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and

(2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down.

(3) A service provider is not liable for wrongful take-down in response to a notification.

No general obligation to monitor

78. (1) When providing the services contemplated in this Chapter there is no general obligation on a service provider to—

(a) monitor the data which it transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to section 14 of the Constitution, prescribe procedures for service providers to—

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Savings

79. This Chapter does not affect—

(a) any obligation founded on an agreement;

(4) Subartikel (1) is nie van toepassing wanneer die ontvanger van die diens onder die gesag of die beheer van die diensverskaffer optree nie.

Inligtingsopsporingsgereedskap

76. 'n Diensverskaffer is nie aanspreeklik nie vir skade deur 'n persoon gely indien die diensverskaffer gebruikers verwys na of koppel aan 'n webbladsy wat 'n skendende databoodskap of skenkende bedrywigheid bevat, deur inligtingopsporingsgereedskap te gebruik, met inbegrip van 'n adresboek, indeks, verwysing, wyser of hiperskakel, indien die diensverskaffer—

(a) nie werklik kennis het dat die databoodskap of 'n bedrywigheid in verband met die databoodskap die regte van daardie persoon skend nie;

(b) nie bewus is van feite of omstandighede waaruit die skendende bedrywigheid of die skendende aard van die databoodskap blyk nie;

(c) nie 'n finansiële voordeel ontvang wat regstreeks aan die skendende bedrywigheid toegeskryf kan word nie; en

(d) die verwysing na of koppeling aan die databoodskap of bedrywigheid verwyder of toegang daartoe ongeskik maak binne 'n redelike tyd nadat hy of sy ingelig is dat die databoodskap of die bedrywigheid wat met die databoodskap verband hou, die regte van 'n persoon skend.

Afhaalkennisgewing

77. (1) By die toepassing van hierdie Hoofstuk moet 'n kennisgewing van onwettige bedrywigheid op skrif wees, moet dit deur die klaer aan die diensverskaffer of sy of haar aangewese agent gerig wees, en moet dit insluit—

(a) die volle name en adres van die klaer;

(b) die skriftelike of elektroniese handtekening van die klaer;

(c) identifisering van die reg wat na bewering geskend is;

(d) identifisering van die materiaal of bedrywigheid wat na bewering die onderwerp van onwettige bedrywigheid is;

(e) die vereiste regstellende optrede wat deur die diensverskaffer ingestel moet word ten opsigte van die klagte;

(f) telefoniese en elektroniese kontakbesonderhede, as daar is, van die klaer;

(g) 'n verklaring dat die klaer te goeder trou optree; en

(h) 'n verklaring deur die klaer dat na sy of haar wete die inligting in die afhaalkennisgewing waar en korrek is.

(2) Enige persoon wat by 'n diensverskaffer kennis gee van onwettige aktiwiteite met die wete dat dit 'n wesenlike wanvoorstelling van die feite is, sal vir skadevergoeding vir die onregmatige verwydering aanspreeklik wees.

(3) 'n Diensverskaffer is nie aanspreeklik vir onregmatige verwydering as gevolg van 'n kennisgewing nie.

Geen algemene verpligting om te moniteer

78. (1) Wanneer die dienste in hierdie Hoofstuk beoog verskaf word, is daar geen algemene verpligting op 'n diensverskaffer om—

(a) die data wat hy of sy versend of berg, te moniteer nie; of

(b) aktief feite of omstandighede te soek wat op 'n onwettige bedrywigheid dui nie.

(2) Die Minister kan, behoudens artikel 14 van die Grondwet, prosedures vir diensverskaffers voorskryf om—

(a) die bevoegde openbare owerhede stiptelik in kennis te stel van beweerde onwettige bedrywighede onderneem of inligting voorsien deur ontvangers van hul dienste; of

(b) inligting wat die identifisering van ontvangers van hul diens moontlik maak, op versoek van die bevoegde owerhede, aan die owerhede te kommunikeer.

Voorbehoudsbepaling

79. Hierdie Hoofstuk raak nie—

(a) enige verpligting wat op 'n ooreenkoms gebaseer is nie;

(*b*) the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law;

(*c*) any obligation imposed by law or by a court to remove, block or deny access to any data message; or

(*d*) any right to limitation of liability based on the common law or the Constitution.

CHAPTER XII

CYBER INSPECTORS

Appointment of cyber inspectors

80. (1) The Director-General may appoint any employee of the Department as a cyber inspector empowered to perform the functions provided for in this Chapter.

(2) A cyber inspector must be provided with a certificate of appointment signed by or on behalf of the Director-General in which it is stated that he or she has been appointed as a cyber inspector.

(3) A certificate provided for in subsection (2) may be in the form of an advanced electronic signature.

(4) When a cyber inspector performs any function in terms of this Act, he or she must—

(*a*) be in possession of a certificate of appointment referred to in subsection (2); and

(*b*) show that certificate to any person who—

(i) is subject to an investigation or an employee of that person; or

(ii) requests to see the certificate.

(5) Any person who—

(*a*) hinders or obstructs a cyber inspector in the performance of his or her functions in terms of this Chapter; or

(*b*) falsely holds himself or herself out as a cyber inspector,

is guilty of an offence.

Powers of cyber inspectors

81. (1) A cyber inspector may—

(*a*) monitor and inspect any web site or activity on an information system in the public domain and report any unlawful activity to the appropriate authority;

(*b*) in respect of a cryptography service provider—

(i) investigate the activities of a cryptography service provider in relation to its compliance or non-compliance with the provisions of this Act; and

(ii) issue an order in writing to a cryptography service provider to comply with the provisions of this Act;

(*c*) in respect of an authentication service provider—

(i) investigate the activities of an authentication service provider in relation to its compliance or non-compliance with the provisions of this Act;

(ii) investigate the activities of an authentication service provider falsely holding itself, its products or services out as having been accredited by the Authority or recognised by the Minister as provided for in Chapter VI;

(iii) issue an order in writing to an authentication service provider to comply with the provisions of this Act; and

(*d*) in respect of a critical database administrator, perform an audit as provided for in section 57.

(2) Any statutory body, including the South African Police Service, with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector to assist it in an investigation: Provided that—

(b) die verpligting van 'n diensverskaffer wat as sodanig optree onder 'n lisensiërings- of ander reguleringsbestel wat by of kragtens 'n wet ingestel is nie;

(c) enige verpligting wat by wet of deur 'n hof opgelê is om toegang tot enige databoodskap te verwyder, te blokkeer of te ontsê nie; of

(d) enige reg tot beperking van aanspreeklikheid gebaseer op die gemene reg of die Grondwet.

HOOFSTUK XII

KUBERINSPEKTEURS

Aanstelling van kuberinspekteurs

80. (1) Die Direkteur-generaal kan enige werknemer van die Departement aanstel as kuberinspekteur wat gemagtig is om die werksaamhede waarvoor in hierdie Hoofstuk voorsiening gemaak word, te verrig.

(2) 'n Kuberinspekteur moet voorsien word van 'n sertifikaat van aanstelling, onderteken deur of namens die Direkteur-generaal, waarin verklaar word dat hy of sy as 'n kuberinspekteur aangestel is.

(3) 'n Sertifikaat waarvoor in subartikel (2) voorsiening gemaak word, kan in die vorm van 'n gevorderde elektroniese handtekening wees.

(4) Wanneer 'n kuberinspekteur enige werksaamheid ingevolge hierdie Wet verrig, moet hy of sy—

(a) in besit wees van 'n sertifikaat van aanstelling in subartikel (2) bedoel; en

(b) daardie sertifikaat toon aan enige persoon wat—

(i) aan 'n ondersoek onderworpe is of 'n werknemer van daardie persoon is; of

(ii) versoek om die sertifikaat te sien.

(5) Iemand wat—

(a) 'n kuberinspekteur by die verrigting van sy of haar werksaamhede ingevolge hierdie Hoofstuk hinder of belemmer; of

(b) homself of haarself valslik voordoen as 'n kuberinspekteur,

is skuldig aan 'n misdryf.

Bevoegdhede van kuberinspekteurs

81. (1) 'n Kuberinspekteur kan—

(a) enige webwerf of bedrywigheid op 'n inligtingstelsel in die openbare domein moniteer en inspekteer en enige onwettige optrede by die toepaslike owerheid aanmeld;

(b) ten opsigte van 'n kriptografiediensverskaffer—

(i) die bedrywighede van 'n kriptografiediensverskaffer ondersoek met betrekking tot sy of haar nakoming of nie-nakoming van die bepalings van hierdie Wet; en

(ii) 'n bevel op skrif aan 'n kriptografiediensverskaffer uitreik om die bepalings van hierdie Wet na te kom;

(c) ten opsigte van 'n waarmerkingsdiensverskaffer—

(i) die bedrywighede van 'n waarmerkingsdiensverskaffer ondersoek met betrekking tot sy of haar nakoming of nie-nakoming van die bepalings van hierdie Wet;

(ii) die bedrywighede ondersoek van 'n waarmerkingsdiensverskaffer wat homself of haarself, of sy of haar produkte of dienste valslik voordoen as geakkrediteer te wees deur die Owerheid of erken te wees deur die Minister soos in Hoofstuk VI bepaal; en

(iii) 'n bevel op skrif aan die waarmerkingsdiensverskaffer uitreik om die bepalings van hierdie Wet na te kom; en

(d) ten opsigte van 'n administrateur van 'n kritieke databasis, 'n oudit doen waarvoor in artikel 57 voorsiening gemaak word.

(2) Enige statutêre liggaam, met inbegrip van die Suid-Afrikaanse Polisiedienst, met magte van inspeksie of deursoeking en inbeslagneming ingevolge enige wet kan aansoek doen om bystand van 'n kuberinspekteur om te help met 'n ondersoek: Met dien verstande dat—

(a) the requesting body must apply to the Department for assistance in the prescribed manner; and

(b) the Department may authorise such assistance on certain conditions.

Power to inspect, search and seize

82. (1) A cyber inspector may, in the performance of his or her functions, at any reasonable time, without prior notice and on the authority of a warrant issued in terms of section 83(1), enter any premises or access an information system that has a bearing on an investigation and—

(a) search those premises or that information system;

(b) search any person on those premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

(c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation;

(d) demand the production of and inspect relevant licences and registration certificates as provided for in any law;

(e) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation;

(f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence;

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;

(h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide him or her with such reasonable technical and other assistance as he or she may require for the purposes of this Chapter; or

(i) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based, have been complied with.

(2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence.

(3) The Criminal Procedure Act, 1977 (Act No. 51 of 1977), applies with the necessary changes to searches and seizures in terms of this Act.

(4) For purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as data messages.

Obtaining warrant

83. (1) Any magistrate or judge may, upon a request from a cyber inspector but subject to the provisions of section 25 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), issue a warrant required by a cyber inspector in terms of this Chapter.

(2) For the purposes of subsection (1), a magistrate or judge may issue a warrant where—

(a) an offence has been committed within the Republic;

(b) the subject of an investigation is—

(i) a South African citizen or ordinarily resident in the Republic; or

(ii) present in the Republic at the time when the warrant is applied for; or

(c) information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and must—

(a) identify the premises or information system that may be entered and searched; and

(a) die versoekende liggaam by die Departement moet aansoek doen om bystand op die voorgeskrewe wyse; en

(b) die Departement dergelike bystand kan magtig op sekere voorwaardes.

Bevoegdheid om te inspekteer, te deursoek en in beslag te neem

82. (1) 'n Kuberinspekteur kan, by die verrigting van sy of haar werksaamhede, te eniger redelike tyd, sonder vooraf kennisgewing en op gesag van 'n lasbrief wat ingevolge artikel 83(1) uitgereik is enige perseel betree of toegang verkry tot 'n inligtingstelsel wat betrekking het op 'n ondersoek en—

(a) daardie perseel of inligtingstelsel deursoek;

(b) enige persoon op daardie perseel deursoek indien daar redelike gronde bestaan om te glo dat die persoon persoonlike besit het van 'n artikel, dokument of rekord wat op die ondersoek betrekking het;

(c) uittreksels neem uit, of afskrifte maak van enige boek, dokument of rekord wat op of in die perseel of in die inligtingstelsel is en wat op die ondersoek betrekking het;

(d) die lewering van toepaslike lisensies en registrasiesertifikate eis en dit inspekteer soos waarvoor in enige wet voorsiening gemaak word;

(e) enige fasiliteite op die perseel wat gekoppel is aan of geassosieer is met die inligtingstelsel en wat op die ondersoek betrekking het, inspekteer;

(f) toegang verkry tot die werking van enige rekenaar of toerusting wat deel vorm van die inligtingstelsel, en enige geassosieerde apparaat of materiaal wat die kuberinspekteur redelike gronde het om te vermoed in verband met enige misdryf gebruik word of gebruik is, en sodanige werking, apparaat of materiaal inspekteer;

(g) enige inligtingstelsel of deel daarvan gebruik of laat gebruik om enige data te soek wat in sodanige inligtingstelsel vervat is of daartoe beskikbaar is;

(h) van die persoon deur wie of ten behoewe van wie die kuberinspekteur redelike gronde het om te vermoed die rekenaar of inligtingstelsel gebruik word of is, of van enige persoon wat in beheer is van, of andersins betrokke is by die werking van die rekenaar of inligtingstelsel vereis om hom of haar te voorsien van die redelike tegniese en ander hulp wat hy of sy vir die doeleindes van hierdie Hoofstuk vereis; of

(i) die navrae doen wat nodig is om vas te stel of die bepalings van hierdie Wet of enige ander wet waarop die ondersoek gebaseer is, nagekom is.

(2) 'n Persoon wat weier om samewerking te verleen of 'n persoon hinder wat besig is met 'n wettige deursoeking en inbeslagneming ingevolge hierdie artikel is skuldig aan 'n misdryf.

(3) Die Strafproseswet, 1977 (Wet No. 51 van 1977), is met die nodige wysigings van toepassing op deursoekings en inbeslagnemings ingevolge hierdie Wet.

(4) By die toepassing van hierdie Wet sluit enige verwysing in die Strafproseswet, 1977, na "perseel" en "artikel" 'n inligtingstelsel sowel as databoodskappe in.

Verkryging van lasbrief

83. (1) 'n Landdros of regter kan, op versoek van 'n kuberinspekteur maar behoudens die bepalings van artikel 25 van die Strafproseswet, 1977 (Wet No. 51 van 1977), 'n lasbrief uitreik wat ingevolge hierdie Hoofstuk deur 'n kuberinspekteur vereis word.

(2) By die toepassing van subartikel (1) kan 'n landdros of regter 'n lasbrief uitreik waar—

(a) 'n misdryf in die Republiek gepleeg is;

(b) die onderwerp van 'n ondersoek—

(i) 'n Suid-Afrikaanse burger is of gewoonlik in die Republiek woonagtig is; of

(ii) in die Republiek aanwesig is op die tydstip dat aansoek om die lasbrief gedoen word; of

(c) inligting ter sake by die ondersoek toeganklik is vanaf die jurisdiksiegebied van die hof.

(3) 'n Lasbrief om te betree, te deursoek en in beslag te neem, kan te eniger tyd uitgereik word en moet—

(a) die perseel of inligtingstelsel wat betree en deursoek kan word, identifiseer; en

(*b*) specify which acts may be performed thereunder by the cyber inspector to whom it is issued.

(4) A warrant to enter and search is valid until—

(*a*) the warrant has been executed;

(*b*) the warrant is cancelled by the person who issued it or in that person's absence, by a person with similar authority;

(*c*) the purpose for issuing it has lapsed; or

(*d*) the expiry of one month from the date on which it was issued.

(5) A warrant to enter and search premises may be executed only during the day, unless the judge or magistrate who issued it, authorises that it may be executed at any other time.

Preservation of confidentiality

84. (1) Except for the purpose of this Act or for the prosecution of an offence or pursuant to an order of court, a person who has, pursuant to any powers conferred under this Chapter, obtained access to any information may not disclose such information to any other person.

(2) Any person who contravenes subsection (1) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding six months.

CHAPTER XIII

CYBER CRIME

Definition

85. In this Chapter, unless the context indicates otherwise—

"access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

Unauthorised access to, interception of or interference with data

86. (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Computer-related extortion, fraud and forgery

87. (1) A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.

(b) vermeld watter handelinge daarkragtens uitgevoer kan word deur die kuberinspekteur aan wie die lasbrief uitgereik is.

(4) 'n Lasbrief om te betree en te deursoek, is geldig totdat—

(a) die lasbrief uitgevoer is;

(b) die lasbrief gekanselleer word deur die persoon wat dit uitgereik het of, in die afwesigheid van daardie persoon, deur 'n persoon met soortgelyke gesag;

(c) die doel waarvoor dit uitgereik is, verval het; of

(d) een maand na die datum waarop dit uitgereik is, verstryk het.

(5) 'n Lasbrief om 'n perseel binne te gaan en te deursoek, kan slegs gedurende die dag uitgevoer word, tensy die regter of landdros wat dit uitgereik het, magtig dat dit op enige ander tyd uitgevoer kan word.

Handhawing van vertroulikheid

84. (1) Behalwe by die toepassing van hierdie Wet of vir die vervolging van 'n misdryf of na aanleiding van 'n hofbevel, mag 'n persoon wat na aanleiding van enige bevoegdhede kragtens hierdie Hoofstuk verleen, toegang tot enige inligting verkry het nie sodanige inligting aan enige ander persoon openbaar nie.

(2) Enige persoon wat subartikel (1) oortree, is skuldig aan 'n misdryf en by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk wat nie ses maande oorskry nie.

HOOFSTUK XIII

KUBERMISDAAD

Woordomskrywing

85. In hierdie Hoofstuk, tensy die samehang anders aandui, beteken—

"toegang" ook die handelinge van 'n persoon wat, nadat hy of sy kennis geneem het van enige data, bewus word van die feit dat hy of sy nie gemagtig is om toegang tot daardie data te hê nie en nogtans voortgaan met toegang tot daardie data.

Ongemagtigde toegang tot, onderskepping van of inmenging met data

86. (1) Behoudens die Wet op die Verbod op Onderskepping en Meeluistering, 1992 (Wet No. 127 van 1992), is 'n persoon wat opsetlik toegang verkry tot enige data, of dit onderskep, sonder magtiging of toestemming om dit te doen, skuldig aan 'n misdryf.

(2) 'n Persoon wat opsetlik en sonder magtiging om dit te doen, inmeng met data op 'n wyse wat veroorsaak dat sodanige data verander, vernietig of andersins oneffektief gemaak word, is skuldig aan 'n misdryf.

(3) 'n Persoon wat enige toestel, met inbegrip van 'n rekenaarprogram of komponent, wat primêr ontwerp is om veiligheidsmaatreëls vir die beskerming van data te oorkom, wederregtelik vervaardig, verkoop, te koop aanbied, vir gebruik verkry, ontwerp, vir gebruik aanpas, versprei of besit, of enige van daardie handelinge verrig met betrekking tot 'n wagwoord, toegangskode of enige ander soortgelyke data, met die opset om sodanige item wederregtelik te gebruik om hierdie artikel te oortree, is skuldig aan 'n misdryf.

(4) 'n Persoon wat enige toestel of rekenaarprogram in subartikel (3) vermeld gebruik om wederregtelik veiligheidsmaatreëls te oorkom wat ontwerp is om sodanige data of toegang daartoe te beskerm, is skuldig aan 'n misdryf.

(5) 'n Persoon wat 'n handeling wat in hierdie artikel beskryf word, verrig met die opset om in te meng met toegang tot 'n inligtingstelsel wat neerkom op 'n ontsegging, met inbegrip van gedeeltelike ontsegging, van diens aan regmatige gebruikers, is skuldig aan 'n misdryf.

Rekenaarverwante afpersing, bedrog en vervalsing

87. (1) 'n Persoon wat enige van die handelinge in artikel 86 beskryf, verrig of dreig om te verrig met die doel om enige onwettige handelsvoordeel te verkry deur te onderneem om sodanige optrede te staak of daarmee op te hou, of deur te onderneem om enige skade aangerig as gevolg van daardie handeling te herstel, is skuldig aan 'n misdryf.

(2) A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

Attempt, and aiding and abetting

88. (1) A person who attempts to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

(2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

Penalties

89. (1) A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.

(2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.

CHAPTER XIV

GENERAL PROVISIONS

Jurisdiction of courts

90. A court in the Republic trying an offence in terms of this Act has jurisdiction where—

(a) the offence was committed in the Republic;

(b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

Saving of common law

91. This Chapter does not affect criminal or civil liability in terms of the common law.

Repeal of Act 57 of 1983

92. The Computer Evidence Act, 1983, is hereby repealed.

Limitation of liability

93. Neither the State, the Minister, nor any employee of the State is liable in respect of any act or omission in good faith and without gross negligence in performing a function in terms of this Act.

Regulations

94. The Minister may make regulations regarding any matter that may or must be prescribed in terms of this Act or any matter which it is necessary or expedient to prescribe for the proper implementation or administration of this Act.

(2) 'n Persoon wat enige van die handelinge in artikel 86 beskryf, verrig met die doel om enige onwettige voordeel te verkry deur te veroorsaak dat vervalste data vervaardig word met die bedoeling dat dit beskou word of dat daar op gehandel word asof dit eg is, is skuldig aan 'n misdryf.

Poging, en hulpverlening

88. (1) 'n Persoon wat probeer om enige van die misdrywe in artikels 86 en 87 bedoel te pleeg, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met die strawwe uiteengesit in artikel 89(1) of (2), na gelang van die geval.

(2) Enige persoon wat aan iemand hulp verleen om enige van die misdrywe in artikels 86 en 87 bedoel te pleeg, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met die strawwe uiteengesit in artikel 89(1) of (2), na gelang van die geval.

Strawwe

89. (1) 'n Persoon wat skuldig bevind is aan 'n misdryf bedoel in artikels 37(3), 40(2), 58(2), 80(5), 82(2) of 86(1), (2) of (3) is strafbaar met 'n boete of gevangenisstraf vir 'n tydperk wat nie 12 maande oorskry nie.

(2) 'n Persoon wat skuldig bevind is aan 'n misdryf bedoel in artikel 86(4) of (5) of artikel 87 is strafbaar met 'n boete of gevangenisstraf vir 'n tydperk wat nie vyf jaar oorskry nie.

HOOFSTUK XIV

ALGEMENE BEPALINGS

Jurisdiksie van howe

90. 'n Hof in die Republiek wat 'n misdryf ingevolge hierdie Wet verhoor, het jurisdiksie waar—

(a) die misdryf in die Republiek gepleeg is;

(b) 'n voorbereidingshandeling vir die misdryf of enige deel van die misdryf in die Republiek gepleeg is, of waar enige gevolg van die misdryf 'n uitwerking in die Republiek gehad het;

(c) die misdryf deur 'n Suid-Afrikaanse burger of 'n persoon met permanente verblyf in die Republiek of deur 'n persoon wat in die Republiek sake doen, gepleeg is; of

(d) die misdryf gepleeg is aan boord van 'n skip of vliegtuig wat in die Republiek geregistreer is of op 'n reis of vlug na of vanaf die Republiek was op die tydstip toe die misdryf gepleeg is.

Voorbehoud van gemenereg

91. Hierdie Hoofstuk raak nie strafregtelike of sivielregtelike aanspreeklikheid ingevolge die gemenereg nie.

Herroeping van Wet 57 van 1983

92. Die Wet op Rekenaargetuienis, 1983, word hiermee herroep.

Beperking van aanspreeklikheid

93. Nóg die Staat, nóg die Minister, of enige werknemer van die Staat is aanspreeklik ten opsigte van enige handeling of late te goeder trou en sonder growwe nalatigheid in die verrigting van 'n werksaamheid ingevolge hierdie Wet nie.

Regulasies

94. Die Minister kan regulasies uitvaardig betreffende enige saak wat ingevolge hierdie Wet voorgeskryf kan of moet word of enige saak wat dit nodig of dienstig is om voor te skryf vir die behoorlike implementering of administrasie van hierdie Wet.

Short title and commencement

95. This Act is called the Electronic Communications and Transactions Act, 2002, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

Kort titel en inwerkingtreding

95. Hierdie wet heet die Wet op Elektroniese Kommunikasies en Transaksies, 2002, en tree in werking op 'n datum wat die President by proklamasie in die *Staatskoerant* bepaal.

SCHEDULE 1

(see section 4(3))

Item	Column A	Column B
1.	Wills Act, 1953 (Act No. 7 of 1953)	11, 12, 13, 14, 15, 16, 18, 19 and 20
2.	Alienation of Land Act, 1981 (Act No. 68 of 1981)	12 and 13
3.	Bills of Exchange Act, 1964 (Act No. 34 of 1964)	12 and 13
4.	Stamp Duties Act, 1968 (Act No. 77 of 1968)	11, 12, 14

BYLAE 1

(kyk artikel 4(3))

Item	Kolom A	Kolom B
1.	Wet op Testamente, 1953 (Wet No. 7 van 1953)	11,12,13,14,15,16,18,19 en 21
2.	Wet op die Vervreemding van Grond, 1981 (Wet No. 68 van 1981)	12 en 13
3.	Wet op Verhandelbare Instrumente, 1964 (Wet No. 34 van 1964)	12 en 13
4.	Wet op Seëlregte, 1968 (Wet No. 77 van 1968)	11, 12, 14

SCHEDULE 2

(see section 4(4))

1.	An agreement for alienation of immovable property as provided for in the Alienation of Land Act, 1981 (Act No. 68 of 1981).
2.	An agreement for the long-term lease of immovable property in excess of 20 years as provided for in the Alienation of Land Act, 1981 (Act No. 68 of 1981).
3.	The execution, retention and presentation of a will or codicil as defined in the Wills Act, 1953 (Act No. 7 of 1953).
4.	The execution of a bill of exchange as defined in the Bills of Exchange Act, 1964 (Act No. 34 of 1964).

BYLAE 2

(kyk artikel 4(4))

1.	'n Ooreenkoms vir die vervreemding van onroerende eiendom soos bepaal in die Wet op Vervreemding van Grond, 1981 (Wet No. 68 van 1981).
2.	'n Ooreenkoms vir die langtermyn huur van onroerende eiendom vir langer as 20 jaar soos bepaal in die Wet op Vervreemding van Grond, 1981 (Wet No. 68 van 1981).
3.	Die verlyding, retensie en voorlegging van 'n testament of kodisil soos omskryf in die Wet op Testamente, 1953 (Wet No. 7 van 1953).
4.	Die verlyding van 'n verhandelbare instrument soos omskryf in die Wet op Verhandelbare Instrumente, 1964 (Wet No. 34 van 1964).

PRINTED BY CREDA COMMUNICATIONS, CAPE TOWN, FOR THE GOVERNMENT PRINTER, PRETORIA, TEL. (012) 334-4507, 334-4511, 334-4509, 334-4515—7000
GEDRUK DEUR CREDA COMMUNICATIONS, KAAPSTAD, VIR DIE STAATSDRUKKER, PRETORIA, TEL. (012) 334-4507, 334-4511, 334-4509, 334-4515—7000