



# Government Gazette Staatskoerant

REPUBLIC OF SOUTH AFRICA  
REPUBLIEK VAN SUID-AFRIKA

Vol. 471

Pretoria, 8 September 2004

**No. 26768**



**AIDS HELPLINE: 0800-0123-22 Prevention is the cure**

---

**CONTENTS • INHOUD***No.**Page  
No.      Gazette  
         No.***GENERAL NOTICE****Communications, Department of***General Notice*

1951	Electronic Communications and Transactions Act (25/2002): Notice inviting comment on proposed guidelines for recognition of industry representative bodies in terms of Chapter XI.....	3	26768
------	--	---	-------

---

---

## GENERAL NOTICE

---

### NOTICE 1951 OF 2004

#### DEPARTMENT OF COMMUNICATIONS

#### **NOTICE INVITING COMMENT ON PROPOSED GUIDELINES FOR RECOGNITION OF INDUSTRY REPRESENTATIVE BODIES IN TERMS OF CHAPTER XI OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002 (ACT NO. 25 OF 2002)**

The Minister of Communications intends to publish Guidelines for Recognition of Industry Representative Bodies in terms of Chapter XI of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).

Interested persons are hereby invited to furnish comments on the proposed guidelines in the Schedule, within 30 days of the date of publication of this notice at the following address:

For attention:      The Senior Manager c/o Alf Wiltz  
                             Legal Services  
                             Department of Communications;

post to:              Private Bag X860  
                             Pretoria  
                             0001;

or deliver to:        First Floor, Block B  
                             iParioli Office Park  
                             399 Duncan Street  
                             Hatfield, Pretoria;

or fax to:             (012) 4278093;

or e-mail to:         alf@doc.gov.za

Please note that comments received after the closing date may be disregarded.

Alf Wiltz can be reached at tel. (012) 4278070/ 8217 for any enquiries.

**SCHEDULE**

**GUIDELINES: RECOGNITION OF  
INDUSTRY REPRESENTATIVE BODIES  
OF INFORMATION SYSTEM SERVICE PROVIDERS**

## **Table of Contents**

<b>Part 1: Best Practice Code of Conduct</b>	<b>6</b>
<b>Part 2: Checklist of Adequate Criteria</b>	<b>24</b>
<b>Part 3: Monitoring and Enforcement</b>	<b>28</b>

## **PART 1**

### **BEST PRACTICE CODE OF CONDUCT**

#### **1 Background**

##### **1.1. Growth of internet and its importance**

The exponential way in which the internet has grown in importance in all spheres of modern life is trite. It is an important phenomenon of modern society touching the lives of everybody in some way or another. The ease of access and relative cheap cost of disseminating information have changed many of the ways in which information is gathered or disseminated today.

This new phenomenon has brought with it new challenges and dangers to previously existing legal rules and mechanisms. For instance the delictual and criminal rules for defamation or the infringement of copyright had been fairly settled before the advent of the internet. Suddenly the application of the rules relating to publishers such as newspapers, journals and even radio and television, did not quite seem fit in respect of parties such as Internet Service Providers ("ISPs" hereinafter) who technically were publishing information, but had very little control over the content which they published on behalf of others. This problem is not a uniquely South African problem, but exists wherever the internet exists.

ISPs play an important role in the provision and availability of internet services to the public at large. However, the potential for delictual and criminal liability under the provisions of the South African common and statutory law was huge and potentially very dangerous for the continued existence of ISPs and the effective functioning of the internet.

This particular problem was recognised by the South African legislature when the Electronic Communications and Transactions Act 25 of 2002 ("the ECT Act" hereinafter) was drafted and specific provision was made for the protection of ISPs in Chapter XI. The objectives of the provisions are to provide protection to responsible ISPs that meet certain minimum criteria broadly described in the ECT Act and to be refined by the Minister of

Communications. These Guidelines provide the minimum requirements, but also provide guidance in respect of best practice that should be the ultimate goal of all responsible ISPs.

## **1.2. Self regulation rather than legislation**

The legislative approach in Chapter XI, as is the case elsewhere in the world, is to place the emphasis for control on self-regulation by the industry rather than directly applicable legislation or government regulation and intervention. It provides that ISPs will receive protection against third party claims where the ISPs activities relate to acting as a mere conduit, the temporary storage of data (caching), hosting or where it provides information location tools. The protection, however, is only available where the following requirements are met:

- (a) The ISP must belong to an Industry Representative Body (IRB) recognised by the Minister of Communications;
- (b) The ISP must have adopted and implemented the Code of Conduct of the IRB;
- (c) The ISP must not be primarily responsible for the creation, sending, manipulation of or linkage to the infringing data; and
- (d) The ISP must timeously respond to a legitimate take-down notice.

The ECT Act also provides protection in the case of a response to a wrongful take-down notice.

The only monitoring or control done by the state in the above process is to ensure that the IRB and its ISPs meet certain minimum requirements laid down in the ECT Act.

The ECT Act is also quite emphatic that there is no general requirement on ISPs to monitor whether its clients are transgressing the law or to monitor data that it transmits or stores. This is simply a realistic approach, taking cognisance of economic and practical realities in the internet environment.

This set of guidelines provides assistance to Industry Representative Bodies and ISPs on the minimum requirements regarded as adequate by the Minister and against which any application for recognition will be measured. It also contains guidelines on what is viewed

as international best practice and the standards that should ultimately be striven for.

## 2 Principles

These guidelines are based on the following Principles:

- 2.1. *Self regulation.* It is preferred that the regulation and control of illegal or unacceptable conduct and content by ISPs and their clients should be exercised by the industry itself rather than the state. There should be a voluntary acceptance of this policy and these standards by the internet industry. This is in conformance with the provisions of the ECT Act.
- 2.2. *Effectiveness.* Any measures put into place by an IRB and its Members should be effective, realistic, practical and achievable with reference to the mischief to be controlled and the objectives of the ECT Act.
- 2.3. *Constitutional values.* The guidelines are based on and consistent with the constitutional values contained in the Constitution of South Africa, Act 108 of 1996, Chapter 2 and more specifically the provisions on human dignity (s 10), privacy (s 14), freedom of belief, religion and opinion (s 15) and freedom of expression (s 16). The basic values underlying a democratic society such as freedom of speech, protection of privacy and informational integrity, legality and the protection of minors should be respected by ISPs and Internet Content Providers (ICPs).
- 2.4. *Minimum standards of professional conduct.* The guidelines specify the minimum mandatory requirements that need to be met, having reference to the objectives of the ECT Act, but they also give guidance as to what is considered international best practice and professional conduct. Compliance with these minimum standards does not necessarily guarantee that conduct will be legal.
- 2.5. *No basis for liability.* Acceptance or subjection to these standards by an ISP will not constitute an independent basis for legal liability other than for compliance purposes and any complaints or disciplinary proceedings of the IRB.
- 2.6. *Preferred standards of conduct.* The preferred standards of conduct specify a higher



standard based on the requirements of the ECT Act as a whole and international best practice and are not mandatory requirements.

- 2.7. *Protection of consumers and public.* Chapter XI of the ECT Act is aimed at providing protection to ISPs, but also at providing effective remedies to affected third parties in respect of unlawful or illegal content or conduct on the internet. The minimum requirements set out below reflect these objectives. The ECT Act also provides other kinds of consumer protection and protection of privacy in Chapters VII and VIII. The preferred standards of conduct include these objectives and provisions. The Department of Communications (DOC) has an obligation in terms of the ECT Act and to the public at large to ensure that IRBs set an acceptable minimum level of professional conduct for their members to qualify for a limitation of liability.
- 2.8. *Law enforcement.* Effective law enforcement is an important part of effectively controlling illegal content and conduct on the internet. Very often this will require the co-operation of ISPs. The mandatory standards of conduct include a commitment to assist authorities in the legitimate investigation of illegal conduct or content and the enforcement of measures to combat such conduct or content.
- 2.9. *No general obligation to monitor (section 78).* These minimum requirements and guidelines are premised on the principle contained in s 78 of the ECT Act, namely that there is no general obligation on ISPs to monitor the conduct or content of their clients, but they also recognise that responsible ISPs should not be allowed to turn a blind eye where they become aware of illegal content or conduct within their sphere of operation and control.
- 2.10. *Accepted industry standards supported.* Where Industry Representative Bodies already require higher standards than would strictly be the case under Chapter XI of the ECT Act, these standards are included in the mandatory minimum requirements as accepted industry standards.
- 2.11. *Equality and technological neutrality.* There should be equality and technological neutrality in the applicable control measures introduced in respect of Internet Service Providers (ISPs), taking into account the advantages provided by Chapter XI of the ECT Act.

2.12. *Fairness.* Requirements should be fair and not adversely affect the economic viability of ISPs.

2.13. *ECT Act as guideline.* The provisions of the ECT Act provide a guideline for acceptable and lawful content and conduct on the internet.

### **3 Objectives and scope**

These guidelines are aimed at:

- 3.1. Ensuring compliance by ISPs and their Industry Representative Bodies with the requirements contained in the ECT Act before the protection of Chapter XI will be granted.
- 3.2. Ensuring that minimum standards of acceptable content and conduct are specified and complied with.
- 3.3. Ensuring that affordable, quick and effective public access to complaints and disciplinary procedures and redress mechanisms is available and that such procedures and mechanisms are fair, unbiased and transparent.
- 3.4. Preventing the illicit or potentially offensive use of the internet.
- 3.5. Ensuring that information and procedures are available to protect minors from potentially harmful content, conduct or exploitation.
- 3.6. Ensuring that complying ISPs receive the protection that they are entitled to.
- 3.7. Increasing the legality, integrity and safety of the internet.
- 3.8. Providing guidelines on higher standards or preferred standards of conduct that the industry should ultimately be aiming at, having regard to the provisions of the ECT Act in general and international best practice.
- 3.9. Ensuring respect for fundamental rights and freedoms and principles governing public order and safety.
- 3.10. Promoting confidence in the use of the internet.
- 3.11. Recognising and supporting industry standards that have already been developed.

#### 4 Definitions

In these guidelines the following terms will have these meanings ascribed to them:

*Cybercrime*: means any conduct on the internet or connected with the internet or internet usages which constitutes a crime in terms of the South African criminal law, including any conduct punishable in terms of Chapter XIII of the ECT Act.

*Data Subject*: means any natural or juristic person from or in respect of whom personal or business information has been requested, collected, collated, processed or stored.

*ECT Act*: means the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).

*Enforcement Authorities*: means any governmental department, body or person in the service of such department or body, who has the power or authority to officially investigate any illegal or unlawful conduct or to enforce any law, including the common law.

*Illegal Content or Conduct*: means any information in respect of which it is illegal or unlawful to create, possess, publish or copy or any conduct that is illegal in terms of the South African common or statutory law.

*IRB*: means Internet Representative Body.

*ISP*: means Internet Service Provider.

*Potentially Harmful Content*: means any information or content which describes, depicts, expresses, or otherwise deals with matters such as sex, bestiality, pornography, exploitation of children, torture, horror, crime, cruelty, or violence in such a manner that the availability of the information is likely to be injurious to the public good or protected groups such as minors. It also includes any information or content that contains anything, which may incite violence, cruelty or hatred on the basis of racial or sexual discrimination, creed or religion or may incite the commitment of any crime. The provision, possession or dissemination of such information need not necessarily be illegal.

*Spam*: means unsolicited commercial communications (as defined in the ECT Act).

## **5 MINIMUM REQUIREMENTS FOR A CODE OF CONDUCT**

### **5.1. Professional Conduct**

- 5.1.1. Members shall at all times conduct themselves in a professional manner in their dealings with the public, clients, other ISPs and the IRB.
- 5.1.2. Members shall be committed to lawful conduct at all times and compliance with all legal requirements.

### **5.2. Standard Terms of Agreement**

- 5.2.1. Members shall have Standard Terms of Agreement that can be accessed from their websites containing all information and terms relevant to their relationship with their clients. Such Standard Terms shall be made available to any potential client prior to the commencement of any service agreement.
- 5.2.2. The Standard Terms shall contain:
- (a) A commitment that the client shall not knowingly create, store or disseminate any illegal content or intentionally conduct itself in an illegal manner in its usage of the Member's services.
  - (b) A commitment that the client shall comply with take-down notices served on it by the Member or any other complainant; if the client is not satisfied that the take-down is legitimate, that it will temporarily take-down the content while the dispute is submitted to the IRB's dispute resolution mechanisms or to a court of law.
  - (c) A condition that the client shall have a prominent reference on its website to the complaints procedure of the Member or the IRB.
  - (d) A guarantee that no material that infringes copyright will knowingly be created, displayed, published or copied by the client.
- 5.2.3. The Standard Terms shall contain a right on the part of the Member to take down any content which it considers illegal or where it has received a take-down notice and where the client refuses to take down the content in question.

- 5.2.4. The Standard Terms shall contain a right on the part of the Member to suspend or terminate the services of any customer that does not comply with these or any other related contractual obligations.

### **5.3. Service levels**

- 5.3.1. Members may not offer or promise service levels which are not reasonably feasible having regard to their technical capabilities, know-how, the area in which the services are to be delivered and other practical restraints.
- 5.3.2. In their dealings with consumers, other businesses and each other, Members shall act professionally, fairly and reasonably.
- 5.3.3. The IRB shall be satisfied that minimum service levels as set out in the ISP's Standard Terms and Conditions are acceptable having regard to the type of service being rendered, the pricing, the area in which the service is being rendered and any other relevant factors. The IRB should publish a guideline for minimum service levels from time to time.

### **5.4. Content control**

- 5.4.1. The content provider is primarily and directly liable for contents provided.
- 5.4.2. There is no general obligation on any Member to monitor the content of its clients, but it is obliged to take action where it becomes aware of any illegal or unlawful content or conduct or potentially illegal or unlawful content or conduct.
- 5.4.3. A Member shall not knowingly carry, transmit, cache, host or provide links to content that it knows is, or reasonably suspects to be, illegal or unlawful, or engage in conduct which is illegal or unlawful.
- 5.4.4. Members shall co-operate with all lawful requests from Enforcement Authorities.
- 5.4.5. Members shall comply with take-down notices unless such notices are obviously frivolous, unreasonable, vexatious or in bad faith.

- 5.4.6. Members shall adhere to the Code of Conduct, the Disciplinary Code and the decisions of the IRB or any of its sub-committees.
- 5.4.7. Where a Member becomes aware of illegal conduct or content, it shall serve a take-down notice on the customer in question, suspend or terminate the customer's services and report the conduct or content to the relevant Enforcement Authority, whichever actions are the most appropriate. In all instances Members shall report such conduct or content and the steps taken to the IRB within a reasonable period of time.
- 5.4.8. Members shall keep a copy or record of all complaints, take-down notices and materials that have been taken down for a period of three years, unless possession of such materials is illegal. In the latter instance such copies should be provided to the relevant Enforcement Authorities.

## **5.5. Consumer protection**

- 5.5.1. Members are committed to honest and fair dealing.
- 5.5.2. Members are committed to promotional and advertising integrity and shall be truthful in all promotional activities and only publish information that is devoid of inaccuracies, ambiguities, exaggerations or omissions about their operations, services and pricing.
- 5.5.3. Members shall comply with all applicable compulsory advertising standards and regulations.
- 5.5.4. Members are committed to co-operation with any legal requests from Enforcement Authorities.

## **5.6. Privacy and Confidentiality Protection**

- 5.6.1. Members shall respect the constitutional right of internet users to personal privacy and privacy of communications.
- 5.6.2. Members shall not deal in or with personal information of data subjects other than for their own needs or with the express prior permission of the data subject.

- 5.6.3. Members shall respect the confidentiality of electronic mail and messaging.
- 5.6.4. Members shall respect the confidentiality of all commercial information of its clients.
- 5.6.5. Members shall only disclose confidential information if obliged to do so in terms of law or with the express prior permission of the data subject.

#### **5.7. Copyright and Intellectual Property Protection**

- 5.7.1. Members shall respect the intellectual property rights of their clients and third parties and shall not knowingly infringe such rights.
- 5.7.2. Members shall contractually require their clients to guarantee that they will not knowingly infringe the intellectual property rights of any third party.

#### **5.8. Spam Protection**

- 5.8.1. Members shall not send or promote the sending of spam and will take reasonable measures to ensure that their networks are not used by others for this purpose.
- 5.8.2. Members must provide a facility for dealing with complaints about spam originating from their networks and must react expeditiously to complaints received.
- 5.8.3. Members shall contractually require their clients to guarantee that they will not send or promote the sending of spam.

#### **5.9. Protection of Minors**

- 5.9.1. Members will take reasonable steps to ensure that they do not offer paid content subscription services to minors without written permission from a parent or guardian.
- 5.9.2. Members undertake to provide internet access clients with information about procedures and software applications that can be used to assist in the control and monitoring of minors' access to Potentially Harmful Content.
- 5.9.3. Members undertake to provide links to information on filtering software and content



labelling systems that can be used to assist in the control and monitoring of minors' access to Potentially Harmful Content.

### **5.10. Cybercrime**

- 5.10.1. Members will take all reasonable measures to prevent unauthorised access to, interception of, or interference with any data.
- 5.10.2. Members shall contractually require their clients to guarantee that they will not access, intercept or interfere with any data whatsoever, unless specifically authorised to do so.
- 5.10.3. Members are committed to co-operation with any legal requests from Enforcement Authorities in their investigation of and enforcement of measures against cybercrime.

### **5.11. Complaints and Take-Down Procedures**

- 5.11.1. Members shall be committed to comply with the take-down requirements as contained in Chapter XI of the ECT Act.
- 5.11.2. Where an ISP is of the opinion that a take-down notice is frivolous, unreasonable, vexatious or in bad faith it should refer the request to its IRB and notify the complainant.
- 5.11.3. Members shall establish a complaints and take-down procedure, which shall be binding on all clients, including the Complaints Procedure of the IRB.
- 5.11.4. The complaints and take-down procedure shall be published and accessible from the Members' websites.
- 5.11.5. Members shall be committed to receive and investigate complaints, including complaints on spam, illegal or unlawful conduct or content, Potentially Harmful Content, objectionable advertising, breaches of privacy and inadequate service delivery.
- 5.11.6. Members shall make all reasonable efforts to resolve complaints by agreement with the complainant and in terms of their complaints procedure. If the complaint cannot be resolved by agreement within a reasonable period of time, the complaint shall be referred to the IRB.



5.11.7. The complaints and take-down procedures shall contain acceptable turn-around periods for dealing with any complaints or take-down notices.

5.11.8. Members shall comply with decisions of the IRB, its Complaints Committee or its Disciplinary Committee.

## **5.12. Disciplinary Procedure**

5.12.1. Members shall be subject to the Complaints Procedure and Disciplinary Code of the IRB in respect of any transgression or non-compliance with the Code of Conduct.

5.12.2. The IRB or its Disciplinary Body shall have the right to receive and investigate any complaint lodged against a Member.

5.12.3. Members shall be obliged to provide their co-operation to the IRB or its Disciplinary Body.

5.12.4. The IRB may refer any complaint received to the Member in question for resolution.

5.12.5. No action in terms of the Disciplinary Code shall be taken against a Member unless a disciplinary hearing has been held in terms of its Disciplinary Code.

5.12.6. In the event that the Disciplinary Body should find that a Member has transgressed the Code of Conduct or failed to comply with its requirements, the Disciplinary Body may take one or more of the following actions against such Member:

- (a) Issue of a take-down notice;  
and in addition
- (b) Issue a reprimand;
- (c) Temporarily expel (suspend) the Member from the IRB subject to conditions which may include a written undertaking from the Member;
- (d) Expel the Member from the IRB;
- (e) Publish details of the identity of the transgressor, the transgression and action taken;
- (f) Report the conduct or content to the relevant Enforcement Authority.

- 5.12.7. The IRB shall retain records of all complaints, disciplinary proceedings and removed material for a period of 3 years, except where possession of the removed material would be illegal. In the latter instance such material shall be provided to the relevant Enforcement Authority.

### **5.13. Monitoring of Compliance**

- 5.13.1. Members shall submit a report of all complaints and steps taken to the IRB within a reasonable period of time after a complaint or take-down notice has been lodged.
- 5.13.2. Members shall submit an annual statement to the IRB confirming their compliance with the Code of Conduct.
- 5.13.3. The IRB shall have the right to investigate the conduct and compliance with the Code of Conduct by Members on its own initiative and to institute disciplinary proceedings if appropriate.

### **5.14. Informational requirements**

- 5.14.1. Members shall prominently display the Membership logo of the IRB, a reference to its Code of Conduct and the contact details for complaint procedures and take-down notices.
- 5.14.2. Members shall provide full identificatory details on their websites, including but not limited to their registered name, electronic contact details, physical address and telephone and fax details.

### **5.15. Review and Amendment**

- 5.15.1. The IRB shall be entitled to review the Code of Conduct from time to time and to amend it where necessary. Such amendments shall be binding on all Members.

## 6 PREFERRED REQUIREMENTS

*NB These requirements are in no way mandatory but comprise of provisions which are in line with international best practice. They provide guidelines in respect of conduct and provisions that are regarded as desirable for responsible ISPs to aim for.*

### 6.1. Professional Conduct

No further requirements are necessary.

### 6.2. Standard Terms of Agreement

The Standard Terms shall contain:

- (a) A commitment that clients shall adhere to the provisions of Chapter VII of the ECT Act (the Consumer Protection Provisions) if applicable.
- (b) A commitment that clients shall adhere to the provisions of Chapter VIII of the ECT Act (the Privacy Provisions) if applicable and that it shall have a privacy policy which is prominently displayed on and accessible from the client's website.
- (c) A commitment that a client shall have adequate safeguards against the accessing of Potentially Harmful Content by minors and other protected groups.

### 6.3. Service levels

- 6.3.1. Members shall make commitment to maintain and provide users with minimum service levels as contained in their Standard Terms and Conditions.
- 6.3.2. A Member shall not be liable for any non-compliance with minimum service levels due to circumstances beyond its control (*force majeure*).
- 6.3.3. Members shall comply with any Code of Practice endorsed by their IRB regarding the transfer of domain names.

- 6.3.4. Members who register domain names for users will inform the user of the terms and conditions on which the domain name is made available to the user, including any conditions of use and restrictions that may apply.
- 6.3.5. Members must offer clients the option of retaining their respective domain names, other than where such domain names are sub-domains of the relevant Member's own name, where clients choose to transfer to another ISP, whether that ISP is a member or not.
- 6.3.6. Members shall provide redirection facilities for a reasonable period of time and at a reasonable cost to clients who change to another ISP.
- 6.3.7. Members should take reasonable steps to respect and implement the caching directions or restrictions of their clients.

#### **6.4. Content control**

- 6.4.1. Members shall have an Acceptable Use Policy that is binding on all their clients.
- 6.4.2. Members shall require their clients to adopt and use a system of content classification or labelling capable of identifying content or services as:
  - (a) Educational or children's content or services and as suitable for children;
  - (b) Potentially Harmful Content, potentially objectionable content or adult services in order that users may restrict or exclude unwanted material by the use of content filter technology or software. Such material shall be preceded by suitable on-screen warnings on the home or title page and access control.
- 6.4.3. Members shall require a commitment from clients that they will not use misleading descriptors in their metatags and advertising.
- 6.4.4. Members shall require a commitment from their clients that they will not contravene the provisions of the Films and Publications Act 65 of 1996.

#### **6.5. Consumer protection**

- 6.5.1. Members shall comply with the provisions of the ECT Act Chapter VII.

- 6.5.2. Members shall not use advertising that is illegal, offensive or deceptive.
- 6.5.3. Members shall not knowingly disseminate information that is false or deceptive.
- 6.5.4. Members shall not knowingly exploit the lack of experience or knowledge of their clients.
- 6.5.5. Members shall have a clear and binding refund and exchange policy.
- 6.5.6. Members shall provide prospective clients with full particulars in respect of size of files, restrictions, operating systems and software required to view or use internet content.
- 6.5.7. Members shall provide prospective clients with full particulars of software licences and conditions when offering software for purchase or use.
- 6.5.8. Members shall provide full details on the identity, professional qualifications and any post occupied by an expert or specialist when offering consultancy services.
- 6.5.9. Members shall give adequate notice of information, data or circumstances that are likely to undergo changes.
- 6.5.10. Members shall contractually require their clients to comply with the ECT Act Chapter VII and all of the above commitments and obligations.

## **6.6. Privacy and Confidentiality Protection**

- 6.6.1. Members shall comply with the provisions of the ECT Act Chapter VIII.
- 6.6.2. Members shall advise users on software tools, which they can use to protect their privacy and integrity of their systems and data.
- 6.6.3. Members shall take reasonable precautions in line with accepted industry practice in the storing of passwords and other confidential information of clients.
- 6.6.4. Members must review the provisions on the prohibition of interception of communications in Chapter 2 of the Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 and implement measures to comply with the those provisions.
- 6.6.5. Members must review the provisions applicable to private bodies in Part 3, Chapters 4

and 5 of the Promotion of Access to Information Act 2 of 2000 and implement measures to comply with those provisions.

- 6.6.6. Members must make their Promotion of Access to Information Act manuals available on the web.
- 6.6.7. Members shall have a Privacy Policy that shall be accessible from their respective websites.
- 6.6.8. Members shall contractually require their clients to comply with the ECT Act Chapter VIII and all of the above commitments and obligations.

#### **6.7. Copyright and Intellectual Property Protection**

Members who offer webpage developing and writing services shall ensure that the ownership of the copyright in any work created for the client, or the terms of the client's licence to use such work, is agreed with the client before work is commenced.

#### **6.8. Spam Protection**

Members shall follow the best industry practice in providing spamming software to clients in order that clients can elect to minimise the amount of spam received on their e-mail accounts.

#### **6.9. Protection of Minors**

No further measures are required. See 6.4 on Content Control above.

#### **6.10. Cybercrime**

- 6.10.1. Members shall take all reasonable steps to prevent cybercrime of any form.
- 6.10.2. Members shall inform their clients and the public about available software and technical measures to protect their information and systems against cybercrime, including hacking

and the spreading of viruses.

6.10.3. Members shall take reasonable measures to establish the identity and physical whereabouts of all clients and to retain records of such information.

6.10.4. Members shall report any illegal or suspected illegal conduct or content to the relevant Enforcement Authority.

6.10.5. Members shall provide a round the clock point of contact to Enforcement Authorities.

#### **6.11. Complaints and Take-Down Procedures**

Members shall provide clients and the public with a round the clock hotline to receive reports on any illegal or unlawful conduct or content and make complaints.

#### **6.12. Informational and educational services**

Members shall be committed to provide public education on internet issues and on the industry, including:

- (a) Information on issues of cybercrime such as hacking, copyright infringement and fraud and available software to prevent or limit cybercrime;
- (b) Information on spam and available software to prevent or limit spam;
- (c) Information on Potentially Harmful Content and available software to prevent or limit access to such content;
- (d) Information on setting up and managing an internet site and the associated costs.

**PART 2****CHECKLIST OF ADEQUATE CRITERIA***ECT Act Section 71**Recognition of representative body**(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that-**(b) membership of the representative body is subject to adequate criteria;*

**All Applications for Membership to the [Name of IRB] shall comply with the following minimum criteria:**

**DOES THE APPLICATION CONTAIN:**

<b>1 Professional conduct</b>	
A commitment to professional and lawful conduct and compliance with all legal requirements?	
<b>2 Standard Terms of Agreement</b>	
Standard Terms of Agreement containing the minimum requirements prescribed?	
<b>3 Service levels</b>	
3.1. A commitment for the provision of well defined service levels that can be accessed from the Member's website?	
3.2. An appraisal of the Member's technical know-how and resources?	
3.3. A commitment to provide service levels which are adequate with reference to industry standards?	
<b>4 Content control</b>	
4.1. A commitment not to knowingly carry, cache, transmit or host content that is illegal or engage in illegal conduct?	



4.2. A commitment to take appropriate action in respect of illegal or unlawful conduct of which it is aware?	
4.3. A commitment to assist Enforcement Authorities in lawful investigations and enforcement?	
4.4. A commitment to adhere to take-down notices?	
4.5. A commitment to store removed materials?	
<b>5 Consumer protection</b>	
5.1. A commitment to honest and fair dealing?	
5.2. A commitment to promotional and advertising integrity and compliance with applicable legislation and regulations?	
<b>6 Privacy and Confidentiality Protection</b>	
6.1. A commitment to respect the privacy of clients and users, their communications and their confidential information?	
6.2. A commitment to use personal information only for purposes authorised by the data subject?	
<b>7 Copyright and Intellectual Property Protection</b>	
7.1. A commitment to respect copyright and other intellectual property rights?	
7.2. A commitment that their clients will contractually agree to respect copyright and other intellectual property rights?	
<b>8 Spam protection</b>	
8.1. A commitment not to send spam and to take reasonable measures to prevent their clients from doing so?	
8.2. A provision for a complaints facility in respect of spam?	

<b>9 Protection of minors</b>	
9.1. A commitment not to offer services to unassisted minors and reasonable measures to prevent this from happening?	
9.2. A commitment to provide access clients with links to or information about filtering and other software to limit or prevent access by minors to Potentially Harmful Content?	
<b>10 Cybercrime</b>	
10.1. A commitment to take reasonable measures against hacking and other forms of cybercrime?	
10.2. A commitment to co-operate with Enforcement Authorities?	
<b>11 Commitment to the Code of Conduct</b>	
A commitment to:	
11.1. Adhere to the provisions of the Code of Conduct of the IRB without exception?	
11.2. Provide information to its clients about the Code of Conduct?	
11.3. Have a clear reference on its website to the Code of Conduct, its membership to the [Name of Industry Representative Body] and the relevant complaints and take-down procedures?	
11.4. Subject itself to the disciplinary code of the [Name of Industry Representative Body] and to comply with any direction from its Disciplinary Body or Board?	
11.5. To comply with take-down requirements as provided for in the ECT Act?	
<b>12 Complaints procedure</b>	
12.1. Provisions for a complaints and take-down procedure available on its website?	
12.2. A commitment to receive and investigate all complaints and to comply with any directions and decisions of the IRB?	
12.3. Acceptable turn-around periods for the resolution of complaints and take-downs?	
12.4. A commitment to be subject to complaints and disciplinary procedures of the IRB?	

<b>13 Monitoring of compliance</b>	
A commitment to comply with the required reporting duties?	
<b>14 Informational requirements</b>	
A commitment to meet the informational requirements stated in 5.14 of the Minimum Requirements for a Code of Conduct.	

### PART 3: MONITORING OF CODE OF CONDUCT

**Act Section 71**

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

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

#### GENERAL

In terms of the ECT Act it is required that the IRB should be capable of monitoring and enforcing its code of conduct in order to receive the necessary recognition (section 71(2)(d)). Effective monitoring and enforcement will firstly be dependent on provisions which are compulsory for all members; secondly a willingness and commitment on the part of the IRB to enforce its Code; and thirdly the financial and human resources to monitor and enforce its Code.

To a large extent the monitoring and enforcement of the Code of Conduct will be reactive rather than proactive, relying on complaints from the public and other interested or affected parties. Because the system will be largely complaints driven, effectiveness will depend heavily on public knowledge of the existence of the Code of Conduct and complaints procedures.

Whether an IRB is capable of doing effective monitoring and enforcing its Code of Conduct will depend on the following aspects:

#### A. Nature and Independence of the IRB

- 1 Consider whether the IRB is appropriately structured and constituted. The following considerations should be taken into account:
  - 1.1. How representative is the IRB of the industry or the industry sector in which it is operating? The more representative the organisation is, the more weight its control and enforcement will carry.
  - 1.2. How independent and unbiased is the IRB in terms of its membership, management and staffing. If it is controlled by a small number of major players, its effectiveness to monitor,

control and enforce the code of conduct could be seriously jeopardised.

1.3. Does the IRB have a proper constitution that makes adequate provision for the following aspects?

- (a) A board or management committee that is regularly elected and can act independently in terms of the Constitution or Articles of Association of the IRB.
- (b) Sufficient staff under the control of the board/ management committee to carry out the functions of the IRB.
- (c) A dispute resolution mechanism?
- (d) A properly constituted complaints and/or disciplinary committee that can act on complaints or transgressions of the Code of Conduct.
- (e) An adequate membership application procedure to screen applications and to ensure that ISPs meet with the minimum requirements required in terms of the constitution or articles of association, membership application requirements and the Code of Conduct.

## **B. Complaints Procedure**

2 The following aspects should be considered when evaluating the Complaints Procedure:

- 2.1. Is there adequate knowledge and awareness of the existence of the Code of Conduct and Complaints Procedures amongst members, their clients and the public? This will depend on whether there is sufficient notice of this information on the respective websites of the ISPs. Does the IRB require its members to make a prominent reference to membership, the Code and complaints procedures on their websites? Is compliance of this checked regularly?
- 2.2. Are there proper record keeping of all complaints received and their resolution, all disciplinary hearings and their results and all appeal proceedings (if any) and their results?
- 2.3. Can the IRB invoke investigations and complaints on its own initiative? Are ISPs compelled to assist in investigations and proceedings?

- 2.4. Are the decisions of complaints and disciplinary committees and the board binding on members?
- 2.5. Are there adequate binding actions or punishments that can be taken against recalcitrant members? Ultimately, are the IRB and its structures entitled to expel the member from the organisation? This remedy effectively removes the protection that the ECT Act provides and is therefore the most severe punishment that can be meted out in this context.
- 2.6. Is there a binding provision for ISPs to notify the IRB of complaints and take-down notices?

### **C. Disciplinary Procedures**

- 3 Does the IRB have an adequate binding disciplinary procedure in terms of its constitution or articles of association if it is not incorporated in the complaints procedure? Essentially the same concerns raised in respect of the complaints procedure should apply to the disciplinary procedure.

### **D. Monitoring Procedures**

- 4 Does the IRB have a policy in place on monitoring and enforcement, including:
  - (f) Procedures for carrying out regular spot checks on sites to check compliance?
  - (g) Procedures for initiating investigations on its own initiative or following on a complaint?
  - (h) Annual detailed compliance statements required from ISPs?
  - (i) Compulsory reporting by ISPs of all complaints and take-down notices received?
- 5 Does the IRB have procedures in place to follow up on complaints and recurring complaints and to check up on compliance with conditions that have been laid down during complaints or disciplinary proceedings or in undertakings made by members?

---

**E. Reporting duties**

- 6 It shall be a condition for continued recognition by the Minister that the IRB shall report any changes to its constitution, articles of association and code of conduct to the Minister.
  - 7 In the event of any such change the Minister shall evaluate the continued eligibility of the IRB for recognition in the light of such changes.
  - 8 It shall be a condition for continued recognition by the Minister that the IRB shall provide an annual report by 28 February to the Minister on:
    - (a) its membership and finances;
    - (b) statistics on complaints and take-down notices received;
    - (c) all disciplinary action taken against members; and
    - (d) any other information the Minister may require from time to time.
-

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001

Publications: Tel: (012) 334-4508, 334-4509, 334-4510

Advertisements: Tel: (012) 334-4673, 334-4674, 334-4504

Subscriptions: Tel: (012) 334-4735, 334-4736, 334-4737

Cape Town Branch: Tel: (021) 465-7531

Gedruk deur en verkrygbaar by die Staatsdrukker, Bosmanstraat, Privaatsak X85, Pretoria, 0001

Publikasies: Tel: (012) 334-4508, 334-4509, 334-4510

Advertensies: Tel: (012) 334-4673, 334-4674, 334-4504

Subskripsies: Tel: (012) 334-4735, 334-4736, 334-4737

Kaapstad-tak: Tel: (021) 465-7531