ISSN0856 – 01001X

THE UNITED REPUBLIC OF TANZANIA

No. 4 *16th August, 2017*

SPECIAL SUPPLEMENT

to the Special Gazette of the United Republic of Tanzania No. 6 Vol. 98 dated 16th August, 2017

Printed by the Government Printer Dar es Salaam by Order of Government

GOVERNMENT NOTICE NO. 287 published on 16/08/2017

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT, (CAP. 306)

THE ELECTRONIC AND POSTAL COMMUNICATIONS (INVESTIGATION) REGULATIONS, 2017

ARRANGEMENT OF REGULATIONS

Regulations *Title*

PART II
INVESTIGATION OF COMMUNICATION

PART III
APPLICATIONS AND EXECUTION OF WARRANT

PART IV
TECHNICAL ADVISORY COMMITTEE

PART V
OBLIGATIONS OF THE AUTHORITY, LAW ENFORCEMENT AGENCIES AND COMMUNICATIONS SERVICE PROVIDERS

PART VII
GENERAL PROVISIONS

THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT,
(CAP.306)

REGULATIONS

(Made under section 165)

THE ELECTRONIC AND POSTAL COMMUNICATIONS
(INVESTIGATION) REGULATIONS, 2017

PART I
PRELIMINARY PROVISIONS

Citation

1. These Regulations may be cited as the Electronic and Postal Communications (Investigation) Regulations, 2017.

Application

2. These Regulations shall apply to Mainland Tanzania as well as Tanzania Zanzibar.

Interpretation

3. In these Regulations, unless the context requires otherwise:

Cap. 306

"Act" means the Electronic and Postal Communications Act;

"apparatus" includes any equipment, machinery or device, any wire or cable;

Cap.172

"Authority" means the Tanzania Communications Regulatory Authority established under the Tanzania Communications Regulatory Authority

Act;

"communications" means anything transmitted by way of electronic or postal service;

"communication service" means any service which includes data, voice, video and all forms of multimedia features consisted in the provision of access to, and of facilities for making use of any communications system including postal services whether or not provided by the person providing the service;

"communication system" means a system existing wholly or partly in the United Republic for the purpose of facilitating the transmission of communications by any means including transmission of post, electronic, electrical or electromagnetic energy or an apparatus comprised thereof;

"Committee" means the Technical Advisory Committee established under regulation 18;

" data" in relation to any communication, means:

(a) any information identifying or purporting to identify any person;

(b) apparatus or location to or from which the communications is or may be transmitted;

(c) any information identifying or selecting, or purporting to identify or select an apparatus by or through which the communication is or may be transmitted;

(d) any information comprising signals for the actuation of the apparatus used for the purposes of a communications system effecting whole or part of the transmission of any communication;

(e) any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

(f) includes any computer data relating to a communication by means of a computer system generated by a computer system that formed a part in the chain of communication indicating the communication's origin, destination, root, time, date, size, duration or type of underlying service; and

(g) content of communication;

"intercept" means listening, monitoring, viewing, tracking, reading or recording by any means, of any private communications;

"intercepted material" means the contents or data of any communication intercepted by an interception to which a warrant relates;

"intercepted subject" in relation to an interception warrant, means a person to whom communication information is sought by the related interception warrant;

"issuing authority" means the Inspector General of Police;

"Minister" has the meaning ascribed to it under the Act;

"postal service" means conventional postal, hybrid postal or courier services;

"protected communications" means an electronic data which requires a key in order to be:

(a) accessible; or

(b) put into an intelligible form; and

''warrant" means an authorization notice or instrument

conferring power to intercept communications.

PART II
INVESTIGATION OF COMMUNICATIONS

Respect to person's right to privacy

4.-(1) Every person's entitlement to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications, shall not be violated.

(2) Without prejudice to sub-regulation (1) any person's communications may be intercepted for the purpose of:

(a) preservation or protection of national security;

(b) preservation of public safety, economic well-being or interest of the country;

(c) the prevention, investigation, or proof of criminal offences; and

(d) prosecution of offenders or the execution of criminal sentences or security measures.

Persons who may intercept

5. -(1) Subject to Regulation 4 interception shall be done by:

(a) the Director General of Tanzania Intelligence and Security Service; or

(b) the Director of Criminal Investigations.

(2) Without prejudice to sub-regulation (1), any person may intercept communications if he:

(a) is a party to the communications;

(b) has the consent of the person who is sending , the person to whom it is sent or a party to the communication;

(c) is authorised by law; or

(d) is bona fide intercepting communications for the purpose of or in connection with the provision, installation, maintenance or repair of the communications service.

Prohibition of interception

6. -(1) A person shall not intercept, attempt to intercept, authorize or procure any other person to intercept or attempt to intercept any communication at any place in the United Republic except as warranted under these Regulations.

(2) A person who contravenes sub regulation (1), commits an offence and shall, on conviction, be liable to a fine of not less than five million shillings or imprisonment for a term of not less than one year or to both.

Possession of interception technology

7.-(1) A person shall not unlawfully develop, possess or attempt to develop or possess an interception technology designed to intercept communication.

(2) A person who contravenes sub regulation (1) commits an offence and shall, on conviction, be liable to a fine of not less than ten million shillings or to imprisonment for a term of not less than two years or to both.

(3) Sub regulation (2), shall not apply to a person who possess an interception technology -

(a) under the direction of an authorized officer in order to assist that officer in the course of his duties under these Regulations; or

(b) for the purpose of fulfilling of obligations in Regulation 5(1) and (2)(d).

(4) For the purpose of this regulation "interception technology" includes any system, device,

(d) is bona fide intercepting communications for the purpose of or in connection with the provision, installation, maintenance or repair of the communications service.

Prohibition of interception

6. -(1) A person shall not intercept, attempt to intercept, authorize or procure any other person to intercept or attempt to intercept any communication at any place in the United Republic except as warranted under these Regulations.

(2) A person who contravenes sub regulation (1), commits an offence and shall, on conviction, be liable to a fine of not less than five million shillings or imprisonment for a term of not less than one year or to both.

Possession of interception technology

7.-(1) A person shall not unlawfully develop, possess or attempt to develop or possess an interception technology designed to intercept communication.

(2) A person who contravenes sub regulation (1) commits an offence and shall, on conviction, be liable to a fine of not less than ten million shillings or to imprisonment for a term of not less than two years or to both.

(3) Sub regulation (2), shall not apply to a person who possess an interception technology -

(a) under the direction of an authorized officer in order to assist that officer in the course of his duties under these Regulations; or

(b) for the purpose of fulfilling of obligations in Regulation 5(1) and (2)(d).

(4) For the purpose of this regulation "interception technology" includes any system, device,

software, equipment or combination of the above crafted to conduct interception.

PART III

APPLICATIONS AND EXECUTION OF WARRANT

Warrant

8. -(1) Where the Director of Criminal Investigations intends to:

(a) intercept communications;

(b) provide, in accordance with an international mutual assistance agreement in criminal matters, an assistance in connection with an interception; or

(c) disclose an intercepted materials obtained through authorized interception,

he shall apply for a warrant from the issuing authority.

(2) An application for a warrant under this regulation shall contain:

(a) the name of the authorized officer and the entity on behalf of which the application is made;

(b) the name, address or profile of the person to be intercepted;

(c) the premises, if any, to which the warrant relates;

(d) the facts or allegations giving rise to the application;

(e) the period of which the warrant is requested;

(f) the nature of equipment in respect of which interception is applied;

(g) a description of the type of communications sought to be intercepted; and

(h) reason for the requirement of the warrant.

(3) The warrant shall contain:

(a) the name, address or profile of the person subjected to interception;
(b) the premises to which the interception warrant relates;
(c) reasons for authorization;
(d) the period for which the warrant is authorized;
(e) the nature of equipment in respect of which interception is authorized;
(f) a description of the type of communications sought to be intercepted;
(g) signature of the issuing authority; and
(h) a statement that the issuing authority has expressly authorised the issue of the warrant.

(4) Where a warrant is produced before any court, purporting to be signed by the issuing authority or on his behalf thereof, it shall be deemed to have been signed by the authorizing authority and may be admitted in evidence.

Effect of warrant

9. -(l) The warrant issued under Regulation (8) shall:

(a) serve as a disclosure order to any person in possession of a key to disclose the protected information to the holder of an interception warrant;
(b) entitle the person in possession of the key to obtain access to the protected communications; and
(c) require the person in possession of the key to disclose the protected communications in an intelligible form.

(2) Where the warrant requires the person to

whom it is addressed to disclose protected communications in terms of paragraph (c), the person shall be presumed to be in compliant with that requirement if he makes a disclosure of any key related to the protected communications that are in his possession.

(4) Where the warrant, which requires an access to a protected communication or the transcription of protected communication into an intelligible form, is addressed to a person who is:

(a) not in possession of the protected communications in relation to such warrant; or

(b) not in possession of the key to permit access to the protected communications,

he shall be deemed to be in compliance with the warrant regardless of inaccessibility of the protected communications.

(5) Where-

(a) the disclosure required by the warrant allows the person to whom it is addressed to comply without disclosing all keys in his possession; and

(b) there are different keys or combination of keys in the possession of that person, the disclosure of which would constitute compliance with the order,

such person may be at liberty to select the keys or combination of keys to be disclosed for the purpose of complying with the warrant.

(6) Where the warrant is addressed to a person:

(a) who was in possession of the key but is no longer in possession of it;

(b) who if he had continued to have the key in his possession, would have been required by virtue of the order to disclose it; and
(c) is in possession of information that would facilitate the obtaining or discovery of the key or transcription of the communications into an intelligible form,

that person shall disclose to the person to whom he would have been required to disclose the key.

Failure to comply with warrant

10. A person who, fails to comply with the terms of the warrant commits an offence and shall, on conviction, be liable to imprisonment for a term of not less than twelve months or to a fine not less than five million shillings or both.

Scope of a warrant

11.- (l) An authorized officer who executes a warrant shall ensure that:

(a) the warrant is used to obtain access to or put the communications in relation to which the warrant was issued in an intelligible form;
(b) any key disclosed pursuant to the warrant is stored in a secure manner;
(c) any records of such key are destroyed as soon as they are no longer needed to access the communications;
(d) the number of:
    (i) persons to whom the key is disclosed or otherwise made available is known; and
    (ii) copies made of the key, is limited to the minimum that is necessary for the purpose of enabling the protected

communication to be accessed or transcribed into an intelligible form.

(2) A warrant issued under these Regulations shall be limited to the subject of communications referred in the warrant and any other person in connection to the said subject's communications.

(3) An authorized officer who contravenes sub regulation (1), commits an offence and shall, on conviction, be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than twelve months or to both.

(4) A person who discloses the existence or contents of a warrant or an application for a warrant, other than to a person to whom such disclosure is authorized, commits an offence and shall, on conviction, be liable to a fine not less than five million shillings or to imprisonment for a term of not less than one year or to both.

Issuing authority

12.-(l) The Inspector General of Police shall be the issuing authority for the purposes of these Regulations.

(2) The issuing authority:

(a) shall be responsible for receiving and processing applications for warrants; and

(b) may, upon satisfaction, issue an interception warrant within twenty four hours.

(3) In the absence of the Inspector General of Police, any person designated by the Inspector General of Police shall be the issuing authority.

Duration of a warrant

13. - (1) The effective period for a warrant shall not exceed ninety days but the issuing authority may

extend the warrant for another period not exceeding ninety days.

(2) Notwithstanding sub regulation (1) the issuing authority may revoke the warrant at any time before it expires.

Modification of Warrant

14. The issuing authority may modify a warrant at any time:

(a) after hearing representations from an authorized officer; and

(b) if he is satisfied that there is any change in the circumstances which constitute grounds for the issuance or renewal of the warrant.

Warrant in urgent circumstances

15.-(1) A person may in urgent circumstances make an oral application to the issuing authority for the issuance of a warrant.

(2) The issuing authority shall, upon receipt of the application in sub regulation (1), consider the application within one hour.

(3) Where the issuing authority is satisfied as to the urgency of the circumstances in sub regulation (1), he may:

(a) dispense with the requirements for a written application and proceed to hear the oral application for the warrant; and

(b) issue a warrant, within one hour.

(4) Where a warrant is issued under this regulation, the applicant shall, within ninety-six hours from the time of issue, submit to the issuing authority the information specified in regulation 8.

(5) The issuing authority may, after expiry of the period specified in sub regulation (4) review his

decision to issue the warrant and:

(a) make an order revoking the warrant if he is not satisfied that the warrant continues to be necessary; or

(b) make an order affirming the warrant, if satisfied that the warrant continues to be necessary.

(6) Where a warrant issued under this regulation is revoked, it shall cease to have effect.

(7) Where a warrant is affirmed under sub regulations (5) (b), regulation 13(1) shall apply with respect to its duration.

(8) Where the applicant fails to comply with sub regulation (2):

(a) the warrant issued under this regulation shall, upon the expiration of ninety-six hours, cease to have effect; and

(b) if the applicant does not give sufficient reason for non compliance , he shall not be allowed to file another application to that effect.

Execution of warrant

16.- (1) An interception warrant issued under these Regulations shall be executed by a person:

(a) to whom it is addressed; or

(b) acting through, or together with other persons as authorised by the warrant.

(2) A person who requires the assistance of any other person to execute an interception warrant shall serve a copy of the warrant to a person whose assistance is sought.

(3) An interception warrant shall be served to a person who:

(a) provides a postal service;

(b) provides a public electronic communications service; or;

(c) who has control of the whole or any part of a communications system located wholly or partly in the United Republic.

(4) A person with respect of whom an interception warrant has been issued under sub regulation (1) shall take all reasonable steps to execute the interception warrant.

(5) A person who fails to comply with sub regulation (4) commits an offence and shall, upon conviction, be liable to a fine not exceeding five hundred thousand shillings or to imprisonment for a term not exceeding two years or to both.

Revocation of a warrant

17.-(1) A warrant issued under these Regulations may be revoked where the issuing authority is:

(a) of the opinion that the warrant is subject to abuse; and

(b) satisfied that the warrant is no longer necessary.

(2) Where a warrant is revoked, the contents of any communications or traffic data intercepted in the course of investigation under that warrant, shall be inadmissible as evidence in any criminal proceedings, unless the Court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice.

Establishment and composition of the

18. - (1) There is established a Committee to be known as the Technical Advisory Committee whose

Technical Advisory Committee

members shall be appointed by the Minister.

(2)The Committee shall be composed of:

(a) the Permanent Secretary from the Ministry responsible for communications, who shall be the Chairman;

(b) one member with relevant technical expertise from the Ministry responsible for communications;

(c) two members with relevant technical expertise from the Authority;

(d) two Law Officers from the Attorney General's Chambers;

(e) one member from the Tanzania Police Force;

(f) one member from the Tanzania Intelligence and Security Service;

(g) one member from any other law enforcement agency designated under regulation 21 (2)(c).

(3) Members of the Committee shall hold office for a term of three years which may be renewed for another term.

(4) The Minister may revoke the appointment of any member of the Committee where he deems proper.

Functions of the Committee

19.- (1) The functions of the Committee shall be:

(a) to advise the Government on technical and operational aspects of interception under these Regulations; and

(b) to perform any other function as may, from time to time, be assigned by the Minister.

(2) A member of the Committee or a person who was a member of the Committee shall not disclose or attempt to disclose to an unauthorized person directly or

indirectly anything which came to his knowledge in the course of discharging his duties as a member of the Committee.

(3) A person who contravenes the sub regulation (2) commits an offence and shall, on conviction, be liable to imprisonment for a term of not less than three years.

PART V
OBLIGATIONS OF THE AUTHORITY, LAW ENFORCEMENT AGENCIES AND COMMUNICATIONS SERVICE PROVIDERS

Obligations of the Authority

20.- (1) The Authority shall have the following responsibilities:

(a) establishing, maintaining and operating a facility within its premises to be known as the Interface Management System;

(b) ensuring that the facility under paragraph (a) is up to date and running all the times;

(c) ensuring the availability of adequate resources to manage the facility; and

(d) monitoring and ensuring that the interface architecture between the law enforcement agencies and the licensees is up and functioning.

(2) In carrying out the obligations under sub regulation (1), the Authority shall not have access to the contents of communications or traffic data passing through the facility.

Obligations of law enforcement agencies

21. (1) A law enforcement agency shall:

(a) establish, maintain and operate a facility within its premises to be known as the

Monitoring Centre;

(b) acquire, install and maintain connections between Interface Management System and the Monitoring Centre; and

(c) ensure availability of adequate resources to manage the facility.

(2) For the purpose of this regulation "law enforcement agency" means:

(a) the Tanzania Police Force;

(b) the Tanzania Intelligence and Security Service; and

(c) any other institution, which the National Security Council may, by a notice in the *Gazette*, designate.

Obligations of communications service providers

22. - (1) A Communication service provider shall ensure that:

(a) its postal or communications systems are technically capable of supporting lawful interceptions at all times;

(b) its services are capable of rendering real time and full time monitoring facilities for the interception of communications;

(c) all call-related information is provided in real-time or as soon as possible upon call termination;

(d) it provides one or more interfaces from which the intercepted communications shall be transmitted to the interface management facility;

(e) intercepted communications are transmitted to the monitoring centre through physical links;

(f) there is proper access to all interception subjects operating temporarily or permanently within their communication systems; and where the interception subject may be using features to divert calls to other service providers or terminal equipment, access to such other providers or equipment;
(g) there is enough capacity to implement simultaneous interceptions;
(h) the identities of monitoring agents and confidentiality of the investigations are safeguarded;
(i) all interceptions are implemented in such a manner that neither the interception target nor any other unauthorized person is aware of any changes made to fulfill the warrant;
(j) registration of all his subscribers or users is as prescribed by the relevant law;
(k) call detail record, internet detail record and any other records of similar nature are kept for a period of not less than six months; and
(l) where a subscriber has unsubscribed himself or has been unsubscribed, registration records of such subscriber are kept for a period of not less than six months.

PART VII
GENERAL PROVISIONS

Admissibility of evidence obtained from an investigation

23. Data obtained in accordance with these Regulations shall be admissible as evidence in any court in accordance with laws relating to admissibility of evidence.

Immunity from legal proceedings

24. No civil or criminal proceedings shall be instituted against a law enforcement officer for any act or omission done in *bona fide* pursuance of his duties.

Offences and penalties

25.- (1) A person who makes a statement under these Regulations which he knows or ought to have known to be false, commits an offence and shall, on conviction, be liable to a fine of not less than one million shillings or to imprisonment for a term of not more than two years or to both.

(2) A person who intentionally discloses the contents or traffic data of any communications obtained by means of a warrant or in a contravention of these Regulations commits an offence and shall, on conviction, be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than twelve months or to both.

(3) A person or service provider who fails to perform a duty or give assistance in terms of these Regulations commits an offence and shall, on conviction,

(a) be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than twelve months or to both; and

(b) be obliged to perform the duty which he failed or omitted to comply within twenty four hours.

Liability of directors and managers of

26. Where a body corporate is convicted of an offence under these Regulations, every person who, at

corporate bodies

the time of commission of the offence was a director, officer or is otherwise concerned with the management of the body corporate is deemed to have committed the same offence unless every such person proves:

(a) that the commission of the offence took place without his consent or knowledge;

(b) that he has exercised due diligence to prevent the commission of the offence; or

(c) that he has exercised due diligence to comply with a lawful order.

Dodoma
14th August, 2017

MAKAME M. MBARAWA
Minister for Works, Transportand Communication