Postal and Telecommunications (Subscriber Registration) Regulations, 2013

ARRANGEMENT OF SECTIONS

Section

IT is hereby notified that the Minister of Transport, Communications and Infrastructural Development has, in terms of section 99 of the Postal and Telecommunications Act [*Chapter 12:05*] and in consultation with the Authority, made the following regulations—

Title and date of commencement

1. (1) These regulations may be cited as the Postal and Telecommunications (Subscriber Registration) Regulations, 2013.

(2) These regulations shall come into operation on the 1st of October, 2013.

Interpretation

2. In these regulations—

"activate" means to allow access to the telecommunication network of the telecommunication service provider;

"address" means—

(a) in the case of a natural person—

(i) the address where the person usually resides, or where such residential address is not available—

(aa) the address where the person is employed; or

(bb) the address where the business of the person is situated;

or

(ii) where such person cannot provide an address contemplated in subparagraph (i), any other address, including that of a school, church or retail store, where the person usually receives his or her post;

or

(b) in the case of a juristic person, the registered address or the address where the business is situated;

"customer" means any person—

(a) to whom a telecommunication service provider provides a telecommunication service, including an employee of the telecommunication service provider or any other person who receives such a service as a gift, donation, favour, reward or benefit;

(b) who has entered in the past or present into a contract with the telecommunication service provider for the provision of a telecommunication service, including a pre-paid, post-paid and telecommunication data service;

"fixed date" means the date fixed under section 1(2) as the date of commencement of these regulations;

"number portability" means the ability of a customer to retain the same telephone number on changing telephone service providers;

"privacy impact form" means a form which evaluates an entire project from a privacy perspective and identifies risks and mitigation strategies throughout;

"service provider" means a telecommunication service provider including cellular and fixed mobile operators, internet access provider and any other telecommunication licensees or designated agents who provides telecommunication services;

"SIM" means Subscriber Identity Module;

"subscriber information" means information or details provided by customers when registering for telecommunication services;

"subscriber identity number" means a SIM card number, data card number or fixed telephone number or any other form of identification provided by a service provider to a customer.

Customer details to be registered

3. (1) No service provider shall activate a SIM-card on its telecommunication network system or provide a telecommunication service unless the customer details have been registered and all the requirements of subsection (4) have been complied with.

(2) Every subscriber of any telecommunication service shall register for the service in terms of subsection (4).

(3) Any subscriber who on the fixed date is not registered with the service provider should ensure that such registration is done within thirty days of the coming into operation of these regulations.

(4) Within thirty days of coming into operation of these regulations all service providers have a duty to deactivate any unregistered subscribers in their networks.

Registration requirements

4. (1) From the date of commencement of these regulations, all service providers must, subject to subsections 9, 10, 11, 12, 13, 14, 15, 16, 17, at their own cost, implement a system to obtain, record and store and must obtain, record and store—

(a) where the customer is a natural person—

(i) their full name; and

(ii) permanent residential address; and

(iii) nationality; and

(iv) gender; and

(v) subscriber identity number; and

(vi) national identification number; or

(vii) passport number;

or

(b) where the customer is a legal person—

(i) copy of certificate of registration or incorporation or business licence; and

(ii) the full names, surname, national identification number and an address of the authorised representative of the legal person; and

(iii) the name and address of the juristic person and, where applicable, the registration number of the legal person; and

(iv) subscriber identity number.

(2) For the purposes of subsection (4), a service provider must verify—

(a) the full names, surname, identity number, address and identity of a customer;

(b) the authority of the representative of the legal person by requiring a letter of authority or an affidavit from the legal person.

(3) Any person who intends to register for a telecommunication service shall submit a copy of a completed registration form to be provided by the service provider to the offices of the service provider or its agent.

(4) All registration forms should contain the information outlined in subsection (1).

(5) Every person should ensure that all information entered into the registration form is true and accurate.

(6) Where there is a change to any of the information submitted to a service provider pursuant to the requirements of subsection (1) a customer shall notify the service provider of such change within 21 days from the occurrence of the change.

(7) If an employee or agent of a service provider knows or suspects that an identification document submitted for verification in terms of subsection (1) is false, he or she must, within 24 hours, report the matter to a police official at any police station.

(8) Any person who provides any information with regard to any details required under this section knowing that such information is false or not having reasonable grounds for believing that such information is true shall be guilty of an offence and liable to a fine not exceeding level five or a period of imprisonment not exceeding six months or to both such fine and such imprisonment.

(9) The information obtained, recorded and stored in terms of subsection (4)must be stored by a service provider for a period of five years after—

(a) a customer has cancelled his or her contract with the service provider; or

(b) the service provider has ended the telecommunication network services provided to the customer.

Keeping of information by persons who lease or offer telecommunication services facilities

5. (1) Any legal person, having complied with section 4 and who provides a SIM-card or access to a fixed telephone or internet service to a person in its employment must, before handing over the SIM-card or providing access to any telecommunication service—

(a) record the particulars as required in section 4 and the date on and period for which the telecommunications service is provided; and

(b) verify—

(i) the full names, surname, identity number and identity of the person to whom the SIM-card is provided; and

(ii) the address.

(2) Any person, having complied with section 4 and who rents a SIM-card, internet or fixed telephone service to another person must, before providing the service to the other person—

(a) record the particulars as required in section 4 and the date on and period for which the telecommunication service is rented; and

(b) verify—

(i) the full names and surname, identity number and identity of the person to whom the telecommunication service is rented; and

(ii) the name and, where applicable, the registration number of the juristic person; and

(iii) the address.

(3) The information provided must be stored for a period of five years.

Conditions attaching to registration

6. (1) Where a mobile phone or SIM card is lost, destroyed or stolen, the owner of that phone or SIM card shall report such loss, theft or destruction in person or through a person duly authorised by him or her to the police and the service provider to whose network the owner subscribed.

(2) Any authorized person, who receives the report provided in subsection (a)shall provide the reporter with written proof of the report which shall be accompanied with a reference number.

(3) Any subscriber has a duty to report any change of ownership of the SIM card, phone number or other identity particulars to the respective service provider.

(4) Any person who possesses a phone number or any subscriber identity number which was previously owned by another person shall have a duty to register that phone number or any subscriber identity information as provided for under section 4.

Obligation of service providers

7. (1) Every service provider shall establish and maintain a register of all subscriber registrations to be known as the Subscriber Register which information provided under section 4 shall be recorded.

(2) Every service provider shall at the request of the Authority, make available a copy of its register or any extract thereof free of charge:

Provided that in the case of the whole register the Authority shall not request more than one hard copy per quarter of a calendar year.

(3) Every service provider shall keep and maintain the register in both material and electronic copy.

(4) Pursuant to sections 4 and 8, every service provider shall ensure that its authorised agents, distributors, or dealers offering telecommunication services shall, within seven (7) days from the date of sale, distribution and registration of any telecommunication service submit to the respective service provider all completed registration forms.

(5) The Authority shall, at reasonable working hours after giving notice to the service provider, be allowed access to the register of a service provider to carry out inspections of records on subscriber registrations to ensure compliance.

(6) Service providers shall maintain subscriber information of customers with numbers or identities ported to other service providers for a period of 5 years.

(7) It shall be the responsibility of the Service Provider to which the number is ported and the customer to comply with the provisions of section 4.

(8) A service provider must, from the date of commencement of this section, inform a customer of—

(a) his or her obligations in terms of section 4; and

(b) the manner in which the obligations must be complied with; and

(c) the consequences of non-compliance.

Establishment of a central subscriber information database

8. (1) The Authority shall establish and maintain a central subscriber information database to be known as the Central Subscriber Information Database, in which all subscriber information shall be stored.

(2) The creation of the database shall enable the Authority to—

(a) monitor service providers' compliance with the provisions of these regulations; and

(b) assist with operation of the emergency call services or assisting emergency services; and

(c) assist law enforcement agencies or safeguarding national security; and

(d) assist with the provision of mobile-based emergency warning systems; and

(e) authorise research in the sector.

(3) Service providers shall, on a monthly basis or at such regular interval as the Authority may from time to time specify, transmit to the Authority all subscriber information captured in their subscriber registers within the preceding month or such period as stipulated by the Authority in accordance with these regulations.

(4) The Authority shall issue guidelines on details of subscriber information to be submitted.

(5) Subject to section 8 the subscriber information contained in the central database shall be held on a strictly confidential basis and no persons or entities shall be allowed access to information on the Central Subscriber Information Database except authorised personnel.

(6) The Authority shall appoint data controllers to take responsibility of such data.

(7) The Authority shall set up mechanisms that will enable data controllers to conduct periodical compliance audits to verify the accuracy of data submitted by service providers.

(8) Data held by the Authority shall be rectified and upgraded from time to time in case of errors and changes in addresses.

(9) Service providers and the Authority shall take all reasonable precautions to preserve the integrity and prevent any corruption, loss or unauthorised disclosure of subscriber information retained pursuant to section 4 and shall take steps to restrict unauthorised use of the subscriber information by its employees who may be involved in the capture and processing of such subscriber information.

(10) Access to any subscriber information stored on the service provider registers and central data base shall be prohibited except on the following grounds–

(a) the operation of the emergency call services or assisting emergency services;

(b) assisting enforcement agencies or safeguarding national security;

(c) the provision of mobile-based emergency warning systems;

(d) undertaking approved educational and research purposes; and

(e) assisting the Authority to verify the accuracy and completeness of information held by licenced operators.

(11) The subscriber information shall not be transferred outside the Republic of Zimbabwe.

(12) In the event of any subscriber information being disclosed in violation of the provisions of these regulations, service providers shall notify the Authority and take reasonable steps to minimise the effect of the breach as soon as practicable upon becoming aware of a substantive or systemic breach of security that could reasonably be regarded as having an adverse impact on the integrity and confidentiality of the protected information.

(13) Any person who is aggrieved by any unlawful use of his or her personal data shall have the right to seek legal redress.

Confidentiality and provision of data for law enforcement purposes

9. (1) A person who is an employee of the Authority, or a service provider or an employee of its agent, dealers or distributors has a duty of confidentiality regarding any information obtained or received in accordance with the provisions of these regulations.

(2) Notwithstanding subsection(1), subscriber information on the Central Data Base may be provided to a law enforcement agent, provided that a prior written request is received by the Authority from an official of the relevant law enforcement agency who is not below the rank of an Assistant Commissioner of Police or a coordinate rank in any other law enforcement agency.

(3) The written notice to be issued by the law enforcement agency pursuant to subsection (2) shall indicate the rank of the official of the law enforcement agent, and the purpose for which the subscriber information is required.

(4) Notwithstanding the foregoing provisions of this section subscriber information shall not be released to law enforcement agencies or any other person, where such release of subscriber information would constitute a breach of the Constitution of the Republic of Zimbabwe, any other enactment or where such release of subscriber information would constitute a threat to national security.

(5) Notwithstanding subsection (2), any authorised person who executes a directive or assists with the execution thereof and obtains knowledge of subscriber information shall only—

(a) disclose such information to a law enforcement officer to the extent that such disclosure is necessary for the proper performance of the official duties of the law enforcement officer; or

(b) use such information to the extent that such use is necessary for the proper performance of his or her official duties.

Provision of data for approved research and educational purposes

10.(1) Persons seeking to use subscriber information for approved research purposes are required to apply to the Authority, specifying the reason for which they seek to use the information.

(2) Applications must be accompanied by a completed privacy impact form.

(3) A research approval is subject to a condition requiring the researcher to make a contractual arrangement to ensure that any contractor to whom the holder discloses protected information neither uses nor discloses the information.

(4) A research approval is subject to a condition prohibiting the researcher from selling or providing customer data to any person for any purpose unless this is authorised.

Secure disposal of protected information after use

11. (1) Any person who is granted the right to use data from the Central Data Base shall securely destroy protected information within 10 working days of—

(a) the protected information no longer being required for the purpose for which it was disclosed to the holder; or

(b) the authorisation ceasing or being revoked.

Penalties

12. (1) Any Service Provider including an agent, distributor or dealer who contravenes or fails to comply with the requirements issued in terms of sections 4, 5, 7, 10, 13, 14, 18, 19 and 20 is guilty of an offence and liable on conviction to a fine not exceeding level 7 for each day on which such failure to comply continues.

(2) Any customer or person who fails to comply with sections 4, 6, 8, 9 and 20 is guilty of an offence and liable on conviction to a fine not exceeding level 5 or a period of imprisonment not exceeding 6 months or to both such fine and such imprisonment.