DATA PROTECTION (COMMUNICATIONS SERVICES) REGULATIONS, 2023

NIGERIAN COMMUNICATIONS ACT, 2003

DATA PROTECTION (COMMUNICATIONS SERVICES) REGULATIONS, 2023

ARRANGEMENT OF REGULATIONS

Regulation:

NIGERIAN COMMUNICATIONS ACT, 2003

DATA PROTECTION (COMMUNICATIONS SERVICES) REGULATIONS, 2023

[*INSERT DATE*]

Commence-ment

In exercise of the powers conferred upon it by section 70 of the Nigerian Communications Act, 2003 and all other powers enabling it in that behalf, the NIGERIAN COMMUNICATIONS COMMISSION hereby makes the following Regulations:

PART I – OBJECTIVE, SCOPE AND APPLICATION OF THESE REGULATIONS

1. These Regulations provide a regulatory framework for the protection and privacy of data in the Nigerian Communications Sector.

Objective.

2. These Regulations relate to the processing of communications data and other categories of data enumerated under the Schedule A to these Regulations.

Scope.

3. The provisions of these Regulations shall apply to –
(a) Licensees;
(b) Subscribers;
(c) Users;
(d) Other third parties directly or indirectly engaged with any of the above in respect of processing of communications data.

Application of these Regulations.

PART II – PROCESSING OF COMMUNICATIONS DATA

4. Every Licensee shall ensure compliance with the following requirements in the processing of communications data:

(a) The basis for processing such data must be provided for under these Regulations, the Act, subsidiary legislations issued by the Commission, or other relevant laws enacted by the National Assembly pertaining to Communications Services;

Requirements for processing Communications Data

(b) Where consent is required before processing communications data, the Licensee must ensure that such consent is specific, informed, unambiguous and given voluntarily;

(c) The purpose for collecting such data must be specified, explicit and legitimate, provided that any further processing of such data must not be incompatible with the initial purpose, apart from the provision of Regulation 36(2) which shall be considered compatible with the initial purposes stipulated under these Regulations;

(d) The data must be relevant and limited to the purpose for which they are processed;

Measures to ensure safety of data

Limitation of processing of Communicat-ions Data.

Persons authorised to process Communica t-ions Data.

Processing of Biometrics Information.

(e) The data processed must be accurate and up to date, provided that licensees shall ensure any inaccurate data are promptly erased or rectified;

(f) Subject to Regulation 36(2), communications data shall not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are processed; and

(g) Appropriate technical and organisational security and measures must be in place to ensure protection of communications data against –

(i) unauthorised and unlawful processing; or
(ii) accidental loss, destruction or damage.

5.–(1) The processing of such data as provided for pursuant to Regulation 2 and the Schedule to these Regulations shall, without prejudice to any other restriction contained in these Regulations, be restricted to what is necessary for the purposes of such activity as is mentioned in sub-regulation (2).

(2) The activities referred to in sub-regulation (1) are activities relating to –

(a) the management of billing or traffic;
(b) customer enquiries;
(c) the prevention or detection of fraud; and
(d) the marketing of any communications services provided by any licensee.

6. Unless the licensee is an individual and the processing is carried out by him personally, processing for the purposes under Regulation 5(2) shall only be carried out by a person –

(a) acting under the authority of the Licensee; and

(b) whose activities under that authority include such activity as is mentioned in Regulation 5(2).

7.–(1) Without prejudice to the provisions of the Registration of Communications Subscribers Regulations, the processing of Biometrics Information for the purposes of uniquely identifying data subjects is prohibited, unless –
(a) the processing is necessary and proportionate for security or authorisation purposes to serve a compelling public interest; and
(b) the Data Subject has given consent, having been provided with a real choice and an alternative.
(2) Notwithstanding sub-regulation (1), transfer of Biometrics Information of data subjects outside the territorial jurisdiction of Nigeria is prohibited.

ONS DATA

8.–(1) Every Licensee shall put in place technical and administrative measures to ensure the safety of its services and communications data. In this regard, a Licensee shall:

PART III – SAFETY OF COMMUNICATI

(a) Develop security policies to ensure the protection of communications data against data breaches that may result in:

(i) unauthorized or unlawful access to such data; or
(ii) damage, loss or disclosure of such data.

(b) The security policies referred to in sub-regulation (1) (a) shall include, but not limited to, provisions relating to: (i) confidentiality, integrity, availability and resilience of the systems used for processing communications data, (ii) prompt restoration and access to communications data in the event of a physical or technical incident occasioning a data breach, (iii) testing, assessment and evaluation of the measures put in place to ensure effective security of the systems used for processing communications data.

(c) Ensure the security of the systems used in storing communications data.

(2) In accordance with the above provisions, the Commission may request information on the measures implemented by the licensee and to require changes to be made to such measures.

9.–(1) A Licensee is required to immediately notify its data subjects where: Data breach.

(a) their personal information has been leaked, in order to prevent secondary damage; or

(b) there is occurrence of risk that threatens their network infrastructure or services.

(2) (a) Notwithstanding the provisions of sub-regulation (1), a Licensee shall promptly report such incident to the Commission and ensure that the breach or risk is remedied as soon as possible, but not exceeding 72 hours from the time of the incident.
(b) Notification of the Commission in the case of a data breach shall contain,
i. the nature of the breach
ii. the consequences of the breach; and
iii. the measures taken or proposed to be taken by the licensee to address the breach.

(3) In relation to sub-regulation (2), the Commission is empowered to investigate the incident and review existing measures put in place by Licensee, in order to forestall the occurrence of any similar incidents, provided that the Commission may impose appropriate sanctions as contained under these Regulations (or any other relevant Regulations of the Commission) where it is discovered that the breach was due to the Licensee's fault.

(4) Every Licensee shall maintain a record of data breaches indicating;
a. the fact surrounding the breach
b. the effect of the breach
c. action(s) taken to remedy the breach

(5) The retention period for the records referred to in sub-regulation (4) shall be in accordance with Regulations 36 and 37 of these Regulations.

PART IV – CONSENT

10.–(1) Notwithstanding any other instances where consent may be required, consent of the Data Subject shall be required for the; Consent requirements.

(a) provisioning of value-added electronic communications services;
(b) marketing of electronic communications services;

(c) publication of telephone numbers in public directories either in print or electronic form.

(2) Provided that no consent shall be required for;

(a) use of traffic data to manage network traffic;
(b) providing interconnections;
(c) use of location data for emergency call management.
(d) Compliance with legal and regulatory obligations

11.–(1) Where consent of a Data Subject is required before processing a communications data, the Data Subject shall be informed of the following; Procedure for obtaining consent.

(a) details of the entity requesting such consent;
(b) the kind of data that will be processed;

(c) how the data will be used; and
(d) the purpose and duration of the processing.

Limitation to use of consent.

(2) The Licensee shall also inform the Data Subject of his right to withdraw such consent at any time.

Where consent is withdrawn.

(3) The consent shall not be implied but must be given expressly, either through a statement or a clear affirmative action which could be written or in electronic form.

(4) Where a data subject is a child or another individual lacking legal capacity to consent, a licensee shall obtain consent of a parent or other appropriate legal guardian of the child or other individual as applicable to rely on consent under Section 10 or 11 hereunder.

(5) A licensee may rely on consent provided by a child aged 13 or more, for the purpose of Section. 10 and 11 in relation to the provision of information and services by electronic means at the individual request of the recipient thereof.

(6) Subsection 11(4) does not apply when:

a. The processing of data is necessary to protect the vital interest of the child or individual lacking the legal capacity to consent.
b. The processing is carried out for purposes of education or medical or social care.
c. The processing is necessary for proceedings before a court relating to the individual.

12. A Licensee shall not make consent compulsory in the form of a pre-condition for the establishment of a subscriber relationship with the Data Subject or for the provision of electronic communication services.

Obligation to keep records of consent

13. Every Licensee is required to maintain and keep an updated database, in print or electronic form, showing the consent of data subjects for the relevant period, without prejudice to the retention period stipulated under Regulation 36 of these Regulations.

Notification of consent periodically

14.–(1) Where a Data Subject has consented to the processing of his data as contained under this Part, the Licensee shall notify the Data Subject, by text message, of the data processing activities carried out pursuant to such consent.

(2) Such notification shall be carried out in the last quarter of each year and a report of all notifications sent shall also be provided to the Commission by each Licensee on or before 31st December of each year.

Responsib-ility to prove consent.

(3) Where a Licensee fails to notify the Data Subject as provided above, any data processing based on such consent must be suspended until notification has been provided.

15.–(1) Any consent obtained lawfully prior to these Regulations shall remain valid, subject to sub-regulation (2).

Consent obtained prior to these Regulations

(2) Where a Data Subject subsequently terminates the subscription for which the consent was previously obtained, the Licensee must immediately discontinue the data processing activities unless consent to continue has been obtained from the Data Subject.

16.–(1) A Data Subject may withdraw any consent given for the processing of his data at any time, and at no cost, by formally notifying the Licensee through its established channels.

(2) Upon receipt of the withdrawal notification, the Licensee shall immediately discontinue the data processing activities for which the consent was initially obtained.

The Licensee has the responsibility of proving that it obtained consent from a Data Subject.

PART V – CALLING AND CALLED LINE IDENTIFICATION

Prevention of calling line identification – outgoing calls.

18. A Licensee shall ensure, where available, that a subscriber originating a call has, subject to Regulations 20 and 21, a simple and free means to withhold his MSISDN from being visible to the called line.

19.–(1) A Licensee shall ensure, where available, that a called subscriber has a simple and free means of preventing the visibility of the MSISDN of the calling subscriber on his line.

Prevention of calling line identification – incoming calls.

(2) Where available, a Licensee shall ensure that a called subscriber has a simple and free means to reject calls from a calling line before the establishment of such calls.

20.–(1) A subscriber originating a call to any national emergency numbers shall not be at liberty to withhold his MSISDN as referred to in Regulation 18.

(2) In relation to calls from national emergency numbers, no person shall be entitled to prevent the visibility of the identity of the calling line on their line as referred to in Regulation 19(1).

National Emergency Calls.

21.–(1) A subscriber shall be entitled to request the tracing of malicious or nuisance calls received on his line, where the identity of the calling line is hidden.

(2) Upon receipt of the application, the Licensee may override any action done to prevent the visibility of the identity of the calling line to the called line, so far as it appears necessary and expedient that the Licensee takes such step.

Tracing of malicious or nuisance calls.

(3) In relation to sub-regulations (1) and (2), nothing in these Regulations shall preclude the Licensee from holding and making available to any Authorised Agencies who makes a written request duly signed by an Authorized Person, data containing the identification of a calling subscriber which were obtained therein, for the purpose of prevention, detection and investigation of a crime.

Request from another Licensee.

22. A Licensee shall comply with any reasonable requests made by another Licensee for the purposes of Regulations 18, 19 and 21.

PART VI – USE OF COMMUNICATIONS SERVICES FOR DIRECT MARKETING PURPOSES

an automated calling system (a syste

23. Without prejudice to the provisions of the Consumer Code of Practice Regulations regarding unsolicited telemarketing, the provisions of this Part shall also apply in respect of processing of data for direct marketing purposes.

24.–(1) A person shall not use, or instigate the use of a publicly available communications service, and a subscriber to such services shall not permit his line to be used by means of

m that operates to make calls without human intervention) for the communication of materials for direct marketing purposes.

Processing of data for direct marketing.

Automated calling systems.

Portability.

Unsolicited calls.

Unsolicited text messages.

Subscriber affected by direct marketing communications.

Application of Part IV.

Supplementary Provisions.

Data

(2) Sub-regulation (1) shall not apply where the called line is that of a subscriber who has previously notified the caller that for the time being, he consents to such communications being sent by or at the instigation of the caller to that line.

25.–(1) A person shall not use, or instigate the use of a publicly available communications service, and a subscriber to such services shall not permit his line to be used for making unsolicited calls, for direct marketing purposes.

(2) Sub-regulation (1) shall also apply where the called line is that of a subscriber who has previously notified the caller that such unsolicited calls should not for the time being be made on that line.

26. A person shall not use, or instigate the use of a publicly available communications service, and a subscriber to such services shall not permit his line to be used for sending unsolicited text messages, for direct marketing purposes, where the subscriber has previously notified the sender that such unsolicited text messages should not be forwarded on that line, for the time being.

27. A subscriber affected by the direct marketing communications referred to under Regulations 24, 25 and 26, who has not consented to receiving such communications, may request his network service provider to place such numbers in a Do Not Disturb (DND) database.

28. The provisions of Part IV shall also apply to Regulations 24, 25 and 26.

29.–(1) Where a publicly available communications service is used for the communication of material for direct marketing purposes –

(2) in the case of an automated calling system or voice call within the meaning of Regulations 24 and 25, the caller shall ensure that the material communicated includes the particulars mentioned in sub-regulation (4).

(3) save as mentioned in sub-regulation (2), such caller or sender shall ensure that the material communicated includes the particulars mentioned in sub-regulation (4)(a) and, if the recipient of the call or text message so requests, those mentioned in sub-regulation (4)(b).

(4) The particulars referred to in sub-regulation (2) are –

(a) the name of the caller or sender; and
(b) either the address of the caller or sender or a phone number on which he can be reached.

PART VII – TRANSFER OF COMMUNICATIONS DATA

30.–(1) Data Subjects shall be entitled to receive a copy of their personal information held by a Licensee upon request.

(2) Sub-regulation (1) shall only apply where –

(a) consent of the Data Subject was the basis relied on by the Licensee for processing the data;

(b) the processing of the personal information is being carried out by automated means, to the exclusion of paper files; or

(c) the request pertains to the personal information the Data Subject provided to the Licensee, but does not extend to any additional data that the Licensee may have created based on the data provided to it by the Data Subject or data about other data subjects.

(3) In transmitting the requested data, the Licensee shall ensure that the data is in a format that is –

(a) structured;
(b) commonly used; and
(c) machine readable.

(4) The Licensee shall comply with a request for data portability without undue delay and at the latest within 30 days of the receipt of the request.

(5) The Licensee shall not charge a fee to comply with a request for data portability.

31.–(1) A Licensee may refuse to comply with a request for data portability by the Data Subject (either wholly or partly) if the request is –

(a) manifestly unfounded; or
(b) excessive.

Refusal to comply with data portability request.

(2) Where a Licensee refuses to comply with a request for data portability, the Data Subject must be informed about –

(a) the reasons for the refusal;
(b) their right to make a written complaint to the Commission; and
(c) their ability to seek to enforce this right through a competent court of jurisdiction.

(3) Sub-regulation (2)(c) shall apply only after the Commission has made a determination pursuant to sub-regulation 2(b), and the Data Subject finds same to be unsatisfactory.

(4) The information stated under sub-regulation (2) shall be provided to the Data Subject not later than 30 days from the receipt of the request.

32.–(1) Data Subjects may request the Licensee to transmit their personal information to a third party.

(2) The request shall be treated on the same terms as already provided for under Regulations 30 and 31, provided the Licensee shall not be responsible

Data transfer to a third party upon request by

Data
Subject.

for any subsequent processing carried out by the Data Subject or the third party on the transmitted data, in so far as the Licensee took appropriate measures to ensure that the data is transmitted securely and to the right destination.

Transfer of Data to a third party.

33. Subject to the provisions of these Regulations, a Licensee may transfer the communications data of a Data Subject to a third party if –

(a) permitted by law; or
(b) consent of the Data Subject is obtained.

Transfer of Data outside Nigeria.

34.–(1) A Licensee shall not transfer data of a Data Subject outside Nigeria unless the data protection regime in the recipient country has been determined by the Commission as providing sufficient and adequate protection for the data to be transferred.

(2) Prior to transferring such data, the Licensee shall request for approval of the Commission, which shall be issued on a case-by-case basis, having due regard to whether the location provides a sufficient level of data protection.

Exemption from approval request.

35. A Licensee shall be exempted from seeking approval from the Commission to transmit data to another country where –

(a) the Data Subject has given prior consent;
(b) the data has been extracted from a public register; or
(c) the transfer is necessary for:

(i) performing a contract with the Data Subject;
(ii) performing a contract with a third party for the benefit of the Data Subject; or
(iii) carrying out a legal obligation.

PART VIII – RETENTION OF COMMUNICATIONS DATA

36.–(1) No communications data shall be retained by a Licensee longer than necessary, having due consideration to the provisions of the Cybercrimes Act as it relates to retention of traffic data and subscriber information.

(2) Notwithstanding sub-regulation (1), a Licensee may keep communications data beyond the stipulated retention period only for archiving, research or statistical purposes, provided approval is obtained in writing from the Commission.

Retention Period.

(3) Where a communications data is no longer needed, the Licensee shall be required to –

(a) erase the data from its live system and any back-up of the data on its system; or
(b) anonymise the data so that it is no longer in a form that makes identification of data subjects possible or reasonably likely.

(4) For the purpose of sub-regulation 3(b), the data must be sufficiently anonymised to the extent that it is irreversibly stripped of any personal identifier of the Data Subject.

(5) Notwithstanding sub-regulation (4), where a Data Subject can still be identified when an anonymised data is combined or matched with other datasets or information available to the Licensee, such will be classified as communications data, further to which the provisions of these Regulations shall apply.

Data retention notice.

37. Notwithstanding Regulation 36, and without prejudice to the provisions of the Cybercrimes Act, the Commission may issue a data retention notice to a Licensee requiring the retention of relevant communications data where it deems it necessary, for one or more of the following purposes:

(a) National security interests;
(b) Prevention, detection and investigation of crimes;
(c) Public safety interests;
(d) Protection of public health; or
(e) Any other purpose in furtherance of the effective regulation of the communications sector as contemplated under the Act.

Considerations for issuance of data retention notice.

38. The Commission may request comments from any Licensee to be affected before issuing a data retention notice, especially in relation to the following considerations:

(a) likely benefits of the notice;
(b) technical feasibility of complying with the notice;
(c) likely number of users or subscribers of the services to be covered by the notice;
(d) likely cost of complying with the notice; and
(e) any other impact the notice might have on the Licensee.

Content of the notice.

39. The data retention notice shall include:

(a) details of the Licensee to which it applies to;
(b) the particular services data is to be retained for;
(c) the data to be retained;
(d) the period for which it should be retained; and
(e) any other information relevant to the retention of the data.

PART IX – SANCTIONS, ENFORCEMENT AND COMPENSATION

Penalties for contravention.

40.–(1) Any Licensee that fails to comply with the provisions of these Regulations shall be liable to an administrative fine of ₦10,000,000.00 and where such an infraction is allowed to continue, such Licensee shall be liable to a daily default penalty of ₦1,000,000.00 until the infraction is either remedied or discontinued.

(2) The Commission, pursuant to the provisions of the Enforcement Processes, Regulations, shall exercise its powers to enforce any sanction imposed under these Regulations.

Right to institute civil proceeding.

41.–(1) A person who suffers damage by reason of any contravention of any of the requirements of these Regulations by any other person may institute a civil proceeding in a court of competent jurisdiction, in order to claim compensation from the other person for that damage.

(2) Sub-regulation (1) shall apply only after the Commission has made a determination in response to a written complaint, and the Data Subject finds same to be unsatisfactory.

PART X – MISCELLANEOUS PROVISIONS

Exemption on grounds of national security.

42. Nothing in any of the provisions of these Regulations shall require a Licensee to do, or refrain from doing, anything, including the processing of data if an exemption of the requirement in question is required for safeguarding national security.

43. Nothing in any of the provisions of these Regulations shall require a Licensee to do, or refrain from doing, anything (including the processing of data) –

(a) if compliance with the requirement in question would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders; or

(b) if exemption from the requirement in question is required for the purposes of, or in connection with, any legal proceedings.

Amendment of Regulations.

44. The Commission may, from time to time, review and modify these Regulations pursuant to its powers under section 72 of the Act.

Powers to issue further directions.

45. The Commission may, from time to time, issue additional rules, directions or guidelines on any aspect of these Regulations.

Interpretation.

Law enforcement and legal requirements.

46. Terms and expressions used, but not defined, in these Regulations shall have the same meaning ascribed to them under the Act or other relevant subsidiary legislations issued by the Commission. In addition, unless the context otherwise requires –

"Act" means the Nigerian Communications Act 2003, as may be amended from time to time;

"Authorised Agencies" shall be as defined in the Lawful Interception of Communications Regulations 2019, as may be amended from time to time;

"Authorised Person" shall be defined as an official of an Authorized Agency not below the rank of an Assistant Commissioner of Police (ACP) or its equivalent.

"Biometrics Information" shall be as defined in the Registration of Communications Subscribers Regulations, as may be amended from time to time;

"Commission" means the Nigerian Communications Commission;

"Communications Data" or *"Data"* shall have the same meaning as contained in the Lawful Interception of Communications Regulations 2019, as may be amended from time to time and shall consist of Traffic Data, Location Data and Personal Information;

"Communications Service" shall be as defined in the Lawful Interception of Communications Regulations 2019, as may be amended from time to time;

"Consent" shall be defined as any voluntary, specific and informed permission communicated expressly by spoken or written words in terms of which a data subject agrees to the processing of personal information relating to the Data Subject

"Consumer Code of Practice Regulations" means the Consumer Code of Practice Regulations, as may be amended from time to time;

"Court" means the Federal High Court of Nigeria;

"Cybercrimes Act" means Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, as may be amended from time to time;

"Data Subject" means a Subscriber and/or a User;

"Enforcement Processes Regulations" means the Nigerian Communications (Enforcement Processes, etc.) Regulations 2019, as may be amended from time to time;

"Licensee" shall be as defined under the Act;

"Location Data" means specific data that determines the geographical location of a device belonging to a public electronic communications service user and is processed in the electronic communications network or through the electronic communications service;

"MSISDN" or *"Line"* means Mobile Station International Subscriber Directory Number or a subscriber's phone number.

"Network Service Provider" shall be as defined in the Act;

"Personal Information" shall be as defined in the Registration of Communications Subscribers Regulations, as may be amended from time to time;

"Processing" means obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, of data fully or partially automatically or non-automatically provided that it is a part of any data recording system. All kinds of operations carried out on the data such as bringing, classifying or preventing its use;

"Registration of Communications Subscribers Regulations" means the Nigerian Communications Commission (Registration of Communications Subscribers) Regulations, as may be amended from time to time.

"Subscriber" shall be as defined in the Registration of Communications Subscribers Regulations, as may be amended from time to time;

"Traffic Data" shall be as defined in the Lawful Interception of Communications Regulations 2018, as may be amended from time to time;

"User" means a person who benefits from the provision of communications services, whether or not they are a subscriber;

Citation.

47. These Regulations may be cited as the Data Protection (Communications Services) Regulations, 2023.

SCHEDULE A *Regulation 2*

SCOPE OF DATA TO BE PROCESSED

These Regulations relate to data which –

1. are in respect of traffic handled by a Licensee;

2. are processed to secure the connection of a call and held by the Licensee concerned;

3. constitute personal information of a Data Subject who is a subscriber to or user of any communications service, or in case of a corporate subscriber or user, would constitute personal information as if that subscriber or user were an individual;

4. are held by a Licensee for purposes connected with the payment of sums due to be paid –

(a) by a subscriber or user; or
(b) by way of interconnection charges.

5. Any other communications data or information as may be determined by the Commission from time to time.

Schedule B - Regulation 8 (1)

MADE at Abuja this [ ] day of [ ], 2023.

PROF. UMAR GARBA DANBATTA, FNSE, FRAES, FAENG, FNIEEE
Executive Vice Chairman
Nigerian Communications Commission

EXPLANATORY NOTE

(This note does not form part of the above Regulations but is intended to explain its purport) These Regulations provide a regulatory framework for the protection and privacy of data in the Nigerian Communications sector.