NATIONAL COMMUNICATIONS AUTHORITY

PUBLIC CONSULTATION

ON

THE PROPOSED REGULATORY FRAMEWORK FOR MANAGEMENT, MONITORING, AND MONETIZATION OF INTERNATIONAL APPLICATION-TO-PERSON (A2P) MESSAGING TRAFFIC IN GHANA

MARCH 2026

NATIONAL COMMUNICATIONS AUTHORITY

INVITATION FOR COMMENTS

1. The National Communications Authority (NCA) intends to introduce a regulatory framework for the management, monitoring, and monetization of international Application-to-Person (A2P) messaging traffic in Ghana.
2. Accordingly, in pursuance of its mandate under Section 3 and Section 25 of the National Communications Authority Act, 2008 (Act 769) and Section 4.1 of the National Telecommunications Policy, 2005 (NTP'05), the Authority hereby invites views and comments from licensees, service providers, financial institutions, technology companies, industry stakeholders and the general public on the proposed framework for the regulation of international A2P messaging services, including the possible introduction of a National A2P Messaging Gateway and associated monitoring and revenue assurance mechanisms.
3. The proposed framework seeks to address challenges associated with limited visibility into international A2P messaging traffic, revenue leakage through unauthorized routing of messaging traffic, and the increasing incidence of fraudulent messaging activities such as spoofing, phishing, and spam campaigns.
4. The consultation document outlines the Authority's proposed regulatory approach and seeks stakeholder input on key issues including:
    - the introduction of a National A2P Messaging Gateway for international messaging traffic;
    - licensing arrangements for an A2P messaging gateway operator;
    - tariff transparency and revenue assurance mechanisms;
    - measures to strengthen consumer protection and messaging security; and
    - safeguards to ensure fair competition and support digital services such as banking and mobile money platforms.
5. The public consultation shall commence with immediate effect and will remain open for four (4) weeks, expiring on **10th April, 2026**.
6. All responses and comments should be submitted electronically as email attachments in Microsoft Word format to info@nca.org.gh, with a copy to **dgsecretariat@nca.org.gh**.
7. Respondents are requested to use the consultation response template annexed to the consultation document when preparing their submissions.
8. It would be helpful if responses clearly indicate the sections of the consultation document with which respondents agree or disagree, together with supporting explanations or evidence where appropriate.

Confidentiality

9. In the interest of transparency and openness, the Authority will treat all submissions as non-confidential and may publish responses received as part of this consultation on its website at **www.nca.org.gh**.
10. Respondents should therefore avoid including confidential or commercially sensitive information in their submissions. Where confidentiality is claimed for

specific information, respondents should clearly identify such information and provide a non-confidential summary where possible.

11. Copyright and all other intellectual property rights in submissions received in response to this consultation shall be deemed to be licensed to the Authority for the purposes of fulfilling its statutory and regulatory responsibilities.

Next Steps

12. Following the conclusion of the consultation period, the Authority will review all submissions received and may engage stakeholders where necessary before issuing the final regulatory framework for the management and regulation of international A2P messaging services in Ghana.

Issued by the Director General
National Communications Authority
10th March, 2026

Executive Summary

Application-to-Person (A2P) messaging has become a critical component of the digital economy. Businesses, financial institutions, government agencies, and digital platforms rely on A2P messaging to deliver automated communications such as one-time passwords (OTPs), transaction alerts, service notifications, and public service announcements.

In Ghana, A2P messaging supports several key sectors including banking and financial services, mobile money platforms, e-commerce services and government digital services. However, the rapid growth of international A2P messaging has introduced regulatory challenges, including:

- limited regulatory visibility into international messaging traffic
- revenue leakage through unauthorized grey routes
- fraudulent messaging activities such as spoofing and phishing
- lack of transparency in A2P pricing structures.

Industry studies indicate that grey route messaging may account for between 15% and 30% of international A2P traffic in emerging markets, resulting in significant revenue losses and security risks.

To address these challenges, the National Communications Authority (NCA) proposes the introduction of a **National A2P Messaging Framework** aimed at improving transparency, strengthening cybersecurity, and enhancing revenue assurance while supporting the continued development of Ghana's digital economy.

The key elements of the proposed framework include:

1. **Introduction of a National A2P Messaging Gateway**

The proposed framework considers the establishment of a centralized gateway that would serve as the primary entry point for international A2P messaging traffic destined for Ghana. This gateway would enable improved monitoring, routing, and reporting of messaging traffic.

2. **Deployment of SMS Firewall Infrastructure**

SMS firewall systems may be deployed within mobile network operator networks to detect and block fraudulent messaging activity, including grey-route traffic, spoofed sender IDs, and SIM-box bypass.

3. **Licensing of a National A2P Gateway Operator**

The Authority proposes to license a neutral infrastructure provider responsible for deploying and operating the gateway infrastructure under regulatory oversight.

4. **Introduction of Transparent Tariff and Revenue Assurance Mechanisms**

The proposed framework may introduce standardized tariff structures and improved reporting mechanisms to enhance transparency in the A2P messaging market.

5. Consumer Protection and Messaging Security

The framework may include enhanced consumer protection measures such as sender ID validation, spam filtering mechanisms, and monitoring of fraudulent messaging campaigns.

6. Safeguards to Address Competition Concerns

The Authority recognizes that centralized infrastructure models may raise competition concerns. Accordingly, safeguards such as competitive licensing, time-bound licences, and regulatory oversight are proposed to ensure that the gateway operates as a neutral infrastructure platform.

Key Consultation Issues

Through this consultation process, the Authority seeks stakeholder views on several key policy issues, including:

1. Whether regulatory intervention is required to address challenges in the international A2P messaging market in Ghana.
2. Whether Ghana should introduce a National A2P Messaging Gateway as part of its regulatory framework.
3. Whether a single gateway operator or multiple gateway operators would be more appropriate for the Ghanaian market.
4. What licensing conditions should apply to the National A2P Gateway operator.
5. Whether standardized tariffs should be introduced for international A2P messaging services.
6. What revenue-sharing arrangements would be appropriate among:
    - mobile network operators
    - gateway infrastructure providers
    - government regulatory institutions.
7. Whether government should introduce a regulatory levy on international A2P messaging traffic.
8. What measures should be implemented to protect consumers from spam, fraudulent messaging, and unauthorized communications.
9. What measures should be introduced to ensure that the regulatory framework does not adversely affect essential messaging services used by banks, fintech companies, and mobile money operators, particularly for authentication messages such as OTPs.
10. What transition period would be appropriate for implementing the proposed framework.

This consultation seeks stakeholder views on the proposed framework before the development of a final regulatory policy.

Table of Contents

1.0 INTRODUCTION

The increasing digitization of economic and social services has significantly expanded the role of telecommunications networks as a platform for automated communications between digital applications and end users.

Application-to-Person messaging enables automated communication between systems and subscribers, providing essential services such as:

- identity authentication
- transaction notifications
- service alerts
- digital service confirmations.

Given its reliability and near-universal reach, A2P messaging has become one of the most effective channels for delivering time-sensitive information. However, the growth of international A2P messaging has introduced regulatory concerns related to:

- traffic monitoring
- consumer protection
- revenue assurance
- network security.

This consultation paper outlines the Authority's proposed framework for addressing these issues.

1.1 Background and Market Context

A2P messaging has become a major component of global digital communications infrastructure. Globally, A2P messaging is used by:

- technology companies
- financial institutions
- e-commerce platforms
- government agencies.

These messages are typically delivered through international messaging aggregators that connect digital service providers to mobile network operators. In many markets, however, unauthorized messaging routes have emerged that bypass official interconnection channels. These grey routes allow traffic to avoid regulatory oversight and termination charges. Such practices undermine market transparency and create vulnerabilities within national telecommunications systems.

1.2 Current A2P Messaging Environment in Ghana

In Ghana, international A2P messaging services are currently delivered through commercial agreements between mobile network operators and international messaging aggregators. While this system allows operators to manage messaging traffic efficiently, it also presents several regulatory challenges including:

Limited Traffic Visibility
The NCA has limited insight into the volume and value of international A2P traffic entering the country.

Revenue Leakage
Unauthorized routing of messaging traffic may lead to loss of legitimate termination revenues.

Security Vulnerabilities
Fraudulent messaging activities such as phishing and spoofing may be facilitated through unregulated messaging channels.

Market Distortion
Operators that comply with regulatory requirements may face unfair competition from entities utilizing unauthorized messaging routes.

1.3 Policy Objectives

The proposed regulatory framework seeks to achieve the following objectives:
Strengthen Regulatory Oversight
Improve visibility into international messaging traffic volumes and routing patterns.

Enhance National Cybersecurity
Reduce the risk of fraudulent messaging and network abuse.

Improve Consumer Protection
Protect subscribers from spam, scams, and unauthorized messaging.

Promote Fair Market Competition
Ensure that all actors within the messaging ecosystem operate under transparent and consistent regulatory conditions.

Enhance Revenue Assurance
Minimize revenue leakage associated with grey-route messaging.

1.4 Legal and Regulatory Framework

The proposed framework is supported by provisions within Ghana's telecommunications regulatory framework.

The Electronic Communications Act, 2008 (Act 775) empowers the Authority to regulate telecommunications networks and services within Ghana. Further, the Electronic Communications (Interconnect Clearinghouse Services) Regulations (L.I. 2234) provide mechanisms for monitoring national and international telecommunications traffic.

The Authority will assess whether additional regulatory instruments may be required to support the implementation of the proposed framework.

2.0 PROPOSED A2P FRAMEWORK

2.1 Policy Options Considered

The Authority has considered several approaches to regulating A2P messaging traffic.

Option 1: Maintain Current Market Structure

This approach would allow existing bilateral agreements between operators and aggregators to continue unchanged. However, this model does not address the challenges associated with traffic visibility and grey-route messaging.

Option 2: Distributed SMS Firewall Model

Under this approach, SMS firewalls would be deployed within individual operator networks to detect fraudulent messaging activity. While this approach improves security, it may not fully address revenue transparency issues.

Option 3: Centralized National A2P Gateway (Proposed Model)

Under this model, international A2P messaging traffic would pass through a centralized gateway that enables traffic monitoring and regulatory oversight.

This model has been implemented in several jurisdictions to strengthen revenue assurance and improve traffic transparency.

2.2 International Benchmarking: Regulation of A2P Messaging Services

Application-to-Person (A2P) messaging has become a globally significant telecommunications service supporting authentication, financial services, e-commerce, and digital government platforms. As A2P messaging volumes have increased, many countries have introduced regulatory frameworks to address challenges associated with:

- grey-route traffic and revenue leakage
- spam and fraudulent messaging
- lack of transparency in international messaging traffic
- consumer protection risks.

These regulatory frameworks typically focus on traffic visibility, revenue assurance, consumer protection, and cybersecurity.

A review of international practices indicates that regulatory approaches generally fall within three broad models: centralized gateway models, distributed firewall systems, and hybrid regulatory monitoring frameworks.

2.2.1 Centralized National Gateway Models

Several countries have implemented centralized gateway systems that act as a national entry point for international A2P messaging traffic. Under this model, international A2P traffic must pass through a regulated gateway that enables:

- monitoring of traffic volumes

- tariff enforcement
- detection of grey-route messaging
- improved revenue assurance.

Nigeria

Nigeria has introduced regulatory initiatives aimed at strengthening oversight of international messaging traffic through enhanced traffic monitoring and anti-grey-route enforcement mechanisms.

These measures are designed to:

- protect telecommunications revenues
- ensure compliance with regulatory requirements
- improve consumer protection against fraudulent messaging.

Tanzania

Tanzania implemented a centralized telecommunications traffic monitoring system that allows regulators to monitor international voice and messaging traffic entering the country. The system enhances regulatory visibility and improves revenue assurance mechanisms.

2.2.2 Distributed SMS Firewall Model

Another widely adopted regulatory approach involves the deployment of **SMS firewalls within individual mobile network operator networks**.

SMS firewalls are designed to detect and block fraudulent messaging activity, including:

- SIM-box bypass
- spoofed sender IDs
- spam messaging campaigns
- grey-route A2P traffic.

India

India has implemented a comprehensive framework for regulating enterprise messaging through the Telecom Regulatory Authority of India (TRAI).

The system includes:

- distributed ledger technology for enterprise messaging
- mandatory sender ID registration
- SMS firewall systems across operator networks.

These measures significantly reduced spam and fraudulent messaging across the country.

2.2.3 Hybrid Regulatory Oversight Model

Some countries adopt hybrid models that combine traffic monitoring with commercial arrangements between operators and international messaging providers.

Under this model, regulators may:

- monitor traffic flows
- establish regulatory guidelines for A2P tariffs
- implement consumer protection measures.

United Arab Emirates

The UAE regulates A2P messaging through licensed messaging aggregators operating under telecommunications regulatory oversight. The framework ensures that international enterprise messaging traffic is delivered through authorized channels.

2.2.4 Key Lessons from International Experience

International experience suggests several important lessons for regulators implementing A2P messaging frameworks.

1. Transparency Improves Revenue Assurance

Countries that introduced traffic monitoring mechanisms reported improved transparency in international messaging traffic volumes.

2. Grey Route Reduction Strengthens Market Integrity

Effective detection and elimination of grey-route messaging helps create a level playing field for licensed operators.

3. Consumer Protection is a Critical Objective

Regulatory frameworks increasingly focus on preventing:

- phishing
- fraud
- spam messaging.

4. Collaboration with Industry is Essential

Successful implementation of A2P regulation requires strong collaboration between:

- regulators
- mobile network operators
- enterprise messaging providers
- digital service platforms.

2.2.5 Implications for Ghana

Based on international experience, the Authority believes that the proposed regulatory framework for A2P messaging in Ghana should aim to:

- improve visibility into international messaging traffic
- enhance cybersecurity protections
- ensure fair monetization of messaging services
- protect consumers from fraudulent messaging activity.

The Authority notes that several countries have successfully implemented regulatory mechanisms to address challenges associated with international A2P messaging.

Ghana's proposed framework seeks to draw on these international best practices while adapting them to the specific characteristics of the Ghanaian telecommunications market. Stakeholders are invited to provide views on the most appropriate international models that Ghana may consider in designing its regulatory framework.

2.3 Proposed Implementation Framework

The Authority proposes the introduction of a National A2P Messaging Gateway Framework comprising the following components.

National A2P Gateway

A centralized gateway will serve as the primary entry point for international A2P messaging traffic.

SMS Firewall Systems

SMS firewall systems will be deployed within mobile operator networks to detect and block unauthorized messaging traffic.

Gateway Operator Licensing

The Authority proposes to license a neutral infrastructure provider responsible for operating the gateway.

Traffic Monitoring and Reporting

The system will provide real-time visibility into messaging traffic volumes and routing patterns.

2.4 Revenue Assurance and Tariff Framework

The consultation seeks stakeholder views on possible approaches to A2P tariff regulation and revenue sharing.

Possible options include:

Option A – Operator-Centric Model

Stakeholder	**Share**
MNOs	70%
Gateway operator	20%
Government	10%

Option B – Balanced Model

Stakeholder	Share
MNOs	60%
Gateway operator	25%
Government	15%

Option C – Regulatory Levy Model

A regulatory levy may be introduced on international A2P traffic while allowing operators to maintain commercial agreements. Rather than revenue sharing, this model introduces a **regulatory levy per message**.

Example structure:

- International A2P termination rate: **USD 0.02per SMS**
- Regulatory levy: **USD 0.002 - 0.004 per SMS**

2.5 Competition and Market Structure Considerations

The Authority recognizes concerns regarding potential monopoly risks associated with centralized infrastructure. To address these concerns:

- the gateway operator will function as a neutral infrastructure provider
- the licensing process will be competitive and transparent
- the licence will be time-bound and subject to regulatory review.

2.6 Impact on Financial Services and Digital Platforms

A2P messaging is widely used by banks, fintech companies, and mobile money operators. To ensure that the proposed framework does not adversely affect essential digital services, the Authority will consider tiered pricing structures that provide preferential pricing for security-related messaging such as OTPs.

2.7 Consumer Protection Measures

Consumer protection mechanisms may include:

- sender ID verification systems
- spam detection tools
- monitoring of fraudulent messaging campaigns
- complaint handling mechanisms.

2.8 Implementation Roadmap

Implementation of the framework will occur in phases:

- Public consultation
- Development of regulatory framework
- Licensing of gateway operator
- Infrastructure deployment and testing
- Migration of international A2P traffic.

2.9 Regulatory Impact Assessment

The Authority has conducted a preliminary assessment of the potential impacts of the proposed framework. Expected outcomes include:

- improved revenue transparency
- enhanced consumer protection
- strengthened cybersecurity
- improved reliability of messaging services.

3.0 LICENSING REQUIREMENTS FOR A2P GATEWAY OPERATOR

3.1 Eligibility Criteria

To ensure the secure, reliable, and efficient operation of the proposed National A2P Messaging Gateway, the Authority proposes to establish a licensing framework for an A2P Messaging Aggregator (National A2P Gateway Operator) responsible for the deployment and operation of the gateway infrastructure.

The licensing framework will seek to ensure that only qualified entities with the necessary **technical, financial, operational, and governance capacity** are authorized to operate this critical national infrastructure.

Applicants seeking to obtain an A2P Messaging Aggregator Licence must meet the following eligibility criteria.

3.2 Legal and Corporate Requirements

Applicants must demonstrate that they are legally constituted entities capable of entering into binding contractual and regulatory obligations. Accordingly, applicants must:

- be a company incorporated under the laws of Ghana, or an external company duly registered to operate in Ghana in accordance with the Companies Act, 2019 (Act 992);
- provide certified copies of incorporation documents, including company registration certificates and constitutional documents;
- demonstrate a clear ownership structure and disclose all beneficial ownership interests;
- provide evidence of tax compliance, including a valid tax clearance certificate issued by the Ghana Revenue Authority;
- demonstrate compliance with all applicable national laws and regulations governing telecommunications, data protection, cybersecurity, and financial reporting.

3.3 Technical Capacity

Applicants must demonstrate the technical capability to deploy, operate, and maintain a national-grade messaging gateway infrastructure capable of handling international A2P traffic across all licensed mobile network operators in Ghana.

Applicants must therefore demonstrate:

- experience in the deployment and management of telecommunications infrastructure, messaging platforms, or related network systems;
- the ability to deploy and operate a secure A2P messaging gateway platform capable of processing high volumes of messaging traffic;

- the technical capability to implement SMS firewall systems capable of detecting and preventing grey-route messaging, spoofing, SIM-box bypass, and other forms of messaging fraud;
- the ability to integrate gateway infrastructure with the networks of all licensed mobile network operators in Ghana;
- the capacity to provide real-time traffic monitoring and reporting systems accessible to the National Communications Authority;
- robust cybersecurity systems designed to protect messaging infrastructure from unauthorized access and cyber threats;
- redundancy and disaster recovery mechanisms to ensure continuity of service.

3.4 Financial Capacity

Applicants must demonstrate sufficient financial capacity to deploy and operate the required gateway infrastructure on a sustainable basis.

Applicants must therefore provide:

- audited financial statements for the past three years, where available;
- evidence of sufficient financial resources to support the capital and operational expenditure required for the deployment and operation of the gateway infrastructure;
- financial guarantees, performance bonds, or other financial instruments demonstrating the applicant's ability to fulfil contractual obligations;
- evidence of access to financing arrangements where necessary.

Where the proposed framework operates under a Build-Operate-Transfer (BOT) model, applicants must demonstrate their ability to finance the deployment and operation of the infrastructure during the licence period.

3.5 Operational and Governance Requirements

Applicants must demonstrate the ability to operate the gateway infrastructure in a transparent and accountable manner consistent with regulatory requirements.
Applicants must therefore demonstrate:

- appropriate governance structures and management capacity;
- internal compliance frameworks to ensure adherence to regulatory obligations;
- operational procedures for monitoring messaging traffic and ensuring compliance with tariff and routing rules;
- mechanisms for cooperation with mobile network operators, international messaging providers, and regulatory authorities;
- internal audit and reporting systems.

3.6 Data Protection and Cybersecurity Compliance

Given the sensitive nature of messaging traffic handled by the gateway infrastructure, applicants must demonstrate full compliance with national data protection and cybersecurity requirements.

Applicants must demonstrate:

- compliance with the Data Protection Act, 2012 (Act 843);
- compliance with the Cybersecurity Act, 2020 (Act 1038);
- secure data storage and processing mechanisms;
- encryption and access control systems designed to protect messaging data;
- procedures for responding to cybersecurity incidents.

3.7 Independence and Conflict of Interest

To promote neutrality and fair market operation, the Authority may impose restrictions on the ownership structure of the gateway operator.

In particular, the Authority may consider:

- restricting ownership by mobile network operators or entities directly controlled by them; or
- imposing safeguards to ensure that the gateway operator functions as a **neutral infrastructure provider** and does not discriminate among market participants.

Stakeholders are invited to provide views on whether mobile network operators should be permitted to participate in the ownership or operation of the gateway infrastructure.

3.8 Local Presence Requirements

To ensure effective regulatory oversight and operational responsiveness, the gateway operator must maintain a **local operational presence in Ghana**.

Applicants must therefore demonstrate:

- the establishment of a local office in Ghana;
- availability of technical and operational staff within Ghana;
- local support capabilities to address operational issues and regulatory requirements.

3.9 Compliance with Licensing Conditions

The successful applicant will be required to comply with all licence conditions issued by the Authority, including obligations relating to:

- service quality standards
- reporting and transparency requirements
- tariff enforcement mechanisms
- consumer protection measures
- cybersecurity compliance.

Failure to comply with licensing conditions may result in regulatory enforcement actions, including suspension or revocation of the licence.

Consultation Issue

The Authority invites stakeholder views on:

- the proposed eligibility criteria for licensing an A2P Messaging Aggregator;
- whether additional technical, financial, or governance requirements should be included; and
- whether mobile network operators should be eligible to participate in the ownership or operation of the gateway infrastructure.

4.0 TERMS AND CONDITIONS FOR A2P GATEWAY OPERATOR LICENCE

The National A2P Messaging Gateway Operator will be subject to a licence issued by the National Communications Authority containing specific operational and regulatory obligations.

4.1 Licence Duration

The Authority proposes that the National A2P Messaging Gateway Operator licence be granted for a period of five (5) years, renewable subject to:

- compliance with regulatory obligations
- satisfactory operational performance
- continued relevance of the regulatory framework.

Stakeholders are invited to provide views on whether a different licence duration may be appropriate.

4.2 Scope of the Licence

The licence will authorize the operator to:

- deploy and operate the National A2P Messaging Gateway infrastructure;
- provide routing and monitoring services for international A2P messaging traffic;
- implement SMS firewall capabilities for traffic monitoring and fraud prevention.

The gateway operator will function strictly as a neutral infrastructure provider and will not provide retail messaging services directly to consumers.

4.3 Service Quality Obligations

The licensee will be required to maintain high levels of service reliability and performance.

Minimum service quality requirements may include:

- system availability of at least 99.99% uptime
- robust redundancy and disaster recovery mechanisms
- rapid response to operational faults or security incidents.

4.4 Reporting and Transparency Obligations

The licensee will be required to provide regular reports to the Authority on:

- messaging traffic volumes
- routing patterns
- tariff compliance
- security incidents or fraud detection.

The gateway platform must also provide real-time monitoring dashboards accessible to the Authority.

4.5 Data Protection and Cybersecurity Obligations

The licensee must comply with all applicable laws relating to data protection and cybersecurity, including:

- the Data Protection Act, 2012 (Act 843);
- the Cybersecurity Act, 2020 (Act 1038).

The licensee must implement appropriate safeguards to ensure the confidentiality and integrity of messaging data.

4.6 Non-Discrimination and Neutrality

The gateway operator must operate the infrastructure on a non-discriminatory basis, ensuring equal treatment of all licensed mobile network operators and authorized messaging providers.

The operator shall not engage in practices that unfairly favour or disadvantage any market participant.

4.7 Regulatory Compliance

The licensee must comply with all regulatory directives issued by the Authority relating to:

- traffic monitoring
- tariff enforcement
- consumer protection
- network security.

Failure to comply with licence conditions may result in enforcement actions including penalties, suspension, or revocation of the licence.

Consultation Issues

Stakeholders are invited to provide views on:

- The proposed methodology for selecting the National A2P Messaging Gateway Operator.
- The proposed licence duration and scope.
- The proposed service quality and reporting obligations.
- Additional safeguards required to ensure neutrality and transparency in the operation of the gateway infrastructure.

5.0 STAKEHOLDER SUBMISSION GUIDELINES AND TIMELINE

Stakeholders are invited to submit written comments addressed to the Director-General via email at info@nca.org.gh or by post with subject: Submission – National A2P SMS Gateway Consultation. All submissions must be received by 10th April, 2026.

Table 1: Timeline for Consultation and Implementation Activities

Activity	Timeline
Publication of Consultation Paper	10th March, 2026
Deadline for Submissions	10th April, 2026
Review and Stakeholder Engagement	20th April– 4th May, 2026
Finalization of Implementation Framework	2nd June, 2026

ANNEX 1 – DEFINITIONS AND ACRONYMS

For the purpose of the present document, the following terms and definitions apply:

A2P SMS: Application-to-Person Short Message Service refers to text messages sent from an application to a mobile subscriber.

Aggregator (National A2P Gateway Operator): The licensed entity responsible for building, financing, and operating the centralized National A2P Gateway and firewall infrastructure, through which all international A2P SMS traffic must be routed.

API: Application Programming Interface is a set of rules and protocols that allows different software applications to communicate with each other.

Firewall (SMS Firewall): A system that monitors, filters, and controls SMS traffic to prevent fraud, spam, revenue leakage and other unauthorized activities.

OTP: One-Time Password is password valid for only one login session or transaction, thus reducing the risk of an unauthorized intruder gaining access to the account.

SMS: Short Message Service is a standard communication protocol for sending text messages between mobile phones.

Spam: Unsolicited or unwanted SMS messages sent via electronic communications technologies such as E-mail, SMS, MMS, or Instant Messaging (IM) to mobile subscribers without explicit opt-in.

ANNEX 2 - CONSULTATION RESPONSE TEMPLATE

Stakeholders are encouraged to use the template below when submitting comments on the Draft Framework for Regulating National Roaming Wholesale Rates.

Respondents may reproduce the table in their submission and provide responses to the consultation questions or other relevant sections of the document.

Stakeholders may also attach additional documents where necessary to provide further analysis or supporting evidence.

Respondent Information

Item	Details
Name of Respondent	
Organisation	
Contact Person	
Position/Title	
Email Address	
Telephone Number	
Date of Submission	

Consultation Response Table

Section of Consultation Document	**Consultation Question / Issue**	**Stakeholder Comment**	**Supporting Evidence or Analysis**	**Proposed Alternative (if any)**

Respondents should clearly indicate the section of the consultation document to which their comments relate.
Stakeholders may provide any additional comments or observations regarding the proposed framework below.

Confidentiality of Submissions

Respondents should indicate whether any part of their submission is confidential.

Confidentiality Status	**Details**
☐ Entire submission is public	

Confidentiality Status	Details
☐ Parts of the submission are confidential	Please identify the confidential sections and provide justification

Where confidentiality is claimed, respondents are encouraged to provide a non-confidential version or summary where possible.

Submission Instructions

Completed submissions should be sent to the Authority within the consultation period specified in the consultation document.

Submissions may be sent electronically to the Authority using the contact details provided in the consultation notice.