



**Malaysian Communications and Multimedia Commission**

# **PUBLIC CONSULTATION PAPER ON UNSOLICITED COMMERCIAL ELECTRONIC MESSAGES**

**Publication date:** 13 August 2025

**Closing date for responses:** 27 August 2025

## TABLE OF CONTENTS

GLOSSARY.....	2
PREFACE .....	3
SECTION 1: BACKGROUND AND POLICY IMPERATIVE.....	4
1.0 Background.....	4
1.1 Problem Statement .....	5
1.2 Rationale for Regulating UCEM.....	6
SECTION 2: INTERNATIONAL BENCHMARKS AND PROPOSED KEY DEFINITIONS.....	8
2.0 International Benchmarking .....	8
2.1 Key Definitions .....	10
SECTION 3: CORE ELEMENTS OF UCEM.....	12
3.0 Malaysian Link.....	12
3.1 Prohibition of Address Harvesting and Dictionary Attacks .....	13
3.2 Consent .....	14
3.3 Mandatory Message Requirements.....	17
SECTION 4: SUBMISSION OF RESPONSES.....	20
ANNEX I: Template For Response .....	21

## GLOSSARY

---

<b>Term</b>	<b>Definition</b>
<b>CASL</b>	Canada's Anti-Spam Legislation
<b>CMA 1998</b>	Communications and Multimedia Act 1998
<b>Commission</b>	Malaysian Communications and Multimedia Commission
<b>GDPR</b>	General Data Protection Regulation
<b>PDPA 2010</b>	Personal Data Protection Act 2010
<b>Regulatory Framework</b>	Regulatory Framework on Unsolicited Commercial Electronic Messages
<b>SMS</b>	Short Messaging Service
<b>UCEM</b>	Unsolicited Commercial Electronic Messages

## PREFACE

The Malaysian Communications and Multimedia Commission (“**the Commission**”) is conducting this Public Consultation to invite feedback on the proposed regulatory framework on Unsolicited Commercial Electronic Messages (“**the Regulatory Framework**”).

A subsidiary legislation will be developed pursuant to the newly inserted Section 233A of the Communications and Multimedia Act 1998 (“**CMA 1998**”), following amendments gazetted in February 2025. The objective is to establish a clear, coherent, and enforceable Regulatory Framework to address the growing issue of unsolicited commercial electronic messages (“**UCEM**”), commonly referred to as spam.

This Public Consultation aims to solicit views from a broad range of stakeholders including industry players, civil society organisations, consumer groups, and members of the public. Feedback is welcomed on policy rationale, the scope of the proposed framework, and the overall regulatory approach. This initiative reflects the Commission’s commitment to transparent, inclusive, consultative, and evidence-based rulemaking process.

The Commission would like to thank all interested parties for their participation and looks forward to receiving constructive feedback through written submissions.

## **SECTION 1: BACKGROUND AND POLICY IMPERATIVE**

### **1.0 Background**

The increasing prevalence of unsolicited commercial electronic messages (“**UCEM**”), commonly known as spam, presents a growing threat to digital trust, user privacy, and national cybersecurity. What was once regarded as a minor nuisance has evolved into a serious concern, often serving as a conduit for scams, phishing attempts, fraud, malware, and other forms of digital exploitation.

Despite the urgency of the issue, Malaysia currently lacks a dedicated and enforceable legal framework specifically tailored to address UCEM. Existing provisions under the Communications and Multimedia Act 1998 (“**CMA 1998**”) are general in scope and do not provide sufficient mechanisms to manage the scale, sophistication, and evolving nature of spam-related activities.

In contrast, jurisdictions such as Canada, Australia, Singapore, and the European Union, have adopted targeted legislative instruments to regulate spam and enhance communication safety. These frameworks serve as valuable benchmarks for the development of Malaysia’s own approach.

To address this gap, the recent amendments to the CMA 1998 introduced a new provision, Section 233A, which expressly prohibits the sending of unsolicited commercial electronic messages. Pursuant to Section 16 of the CMA 1998, the Minister is empowered to make regulations on UCEM, that will be enforced by the Commission.

This Public Consultation seeks feedback on the proposed Regulatory Framework. The framework outlines key principles, regulatory approaches, and compliance considerations, drawing from international best practices and tailored to Malaysia’s enforcement context. It aims to ensure clarity, support compliance, and promote a safer, more trusted online environment.

## 1.1 Problem Statement

The global proliferation of UCEM has become a significant digital threat. These messages, typically promotional in nature, are often sent without the recipient's consent and increasingly serve as vectors for fraudulent schemes and malicious activities. In Malaysia, UCEM is commonly disseminated via email, Short Messaging Service ("**SMS**"), internet messaging services, and social media platforms. They often contain misleading marketing content or hyperlinks that direct users to harmful websites.

The Commission has observed a significant rise in complaints concerning deceptive marketing practices, fraudulent SMS and email campaigns, and other forms of unsolicited electronic messages. A large proportion of these complaints involve the unauthorised use of personal data and numbering resources, aggravating risks to user privacy and safety.

Commission data reveals that reported UCEM related complaints rose by nearly 200% between 2021 and 2025, highlighting a sharp and troubling trajectory. The growing scale and impact of UCEM in Malaysia are reflected in the following key data points:

<b>Type of Spam</b>	<b>Cases (Since 2022)</b>
<b>Phishing</b>	3,168 cases were reported in 2023 <sup>1</sup>
<b>Fraudulent SMS Messages</b>	5.29 million cases were recorded in 2024 <sup>2</sup>
<b>Direct Messaging, Comment Spam, and Fake Accounts</b>	63,652 pieces of fraudulent content were removed from social media platforms in 2024 by the Commission <sup>3</sup>
<b>Reported Spam Cases</b>	Commission data shows a sharp increase in spam complaints between 2021 and 2025, with reported cases rising by nearly 200% over the five-year period.
<b>Email-Based Phishing Attacks</b>	Kaspersky Labs reported over 43 million email-based phishing attacks across Southeast Asia in 2022, with 40% targeting Vietnam, Malaysia, Thailand, and Indonesia <sup>4</sup>

<sup>1</sup> Report: Scam calls in Malaysia skyrocketed by 82.81% in 2024 | The Star

<sup>2</sup> Report: Scam calls in Malaysia skyrocketed by 82.81% in 2024 | The Star

<sup>3</sup> BERNAMA - 63,652 Fraudulent Content Removed From Social Media By MCMC Last Year

<sup>4</sup> Phishing Attacks Rise Sharply in Southeast Asia

Regardless of the transmission medium, whether email, SMS, messaging applications, or social media, UCEM undermines consumer trust, compromises data protection, and weakens the integrity of Malaysia's digital ecosystem. The widespread and persistent nature of these messages increases public exposure to scams, identity theft, malware, harassment, and misinformation.

The growing volume and impact of UCEM underscore the urgent need for a dedicated regulatory response. The harms are multifaceted, ranging from privacy violations and financial loss to reputational damage and exploitation of vulnerable users. These risks necessitate a proactive, rights-based, and enforceable policy approach.

A dedicated legal framework to regulate UCEM is therefore essential to strengthen consumer protection, safeguard national digital infrastructure, enable effective regulatory enforcement and restore public confidence in digital communication channels.

## **1.2 Rationale for Regulating UCEM**

The alarming rise in UCEM related cases highlights a critical regulatory gap in managing the growing risks posed by unsolicited electronic messages. The scale, sophistication, and impact of such activities have outpaced Malaysia's existing legislative tools, warranting the need for a comprehensive and enforceable framework.

Consumer protection lies at the heart of this need. UCEM exposes users to privacy violations, scams, phishing attempts, and fraudulent schemes. A dedicated Regulatory Framework would empower individuals with greater control over their electronic communications and reduce their exposure to harmful and intrusive messages.

From an enforcement perspective, UCEM is a well-established vector for cyber threats. A robust framework will strengthen the Commission's ability to act against malicious actors, support national cybersecurity efforts, and ensure that enforcement mechanisms remain agile and effective.

There is also a need for global alignment. Jurisdictions such as Canada, Australia, the European Union, and Singapore have implemented clear regulatory measures to address spam and protect users. Aligning Malaysia's approach with international best practices will facilitate cross-border cooperation, improve regulatory coherence, and strengthen Malaysia's standing in the global digital ecosystem.

For industry stakeholders, regulation offers clarity and certainty. By establishing clear standards and obligations for businesses engaged in electronic marketing, the framework will promote fair competition and a level playing field for all market participants.

In summary, regulating UCEM is not only necessary to address existing harms, but also a forward-looking measure to ensure that Malaysia's digital ecosystem remains secure, trusted, and inclusive. The proposed Regulatory Framework aims to lay the foundation for a future ready regulatory approach, and the Commission welcomes stakeholder input to refine and strengthen it.

## **SECTION 2: INTERNATIONAL BENCHMARKS AND PROPOSED KEY DEFINITIONS**

### **2.0 International Benchmarking**

This section outlines the regulatory approaches adopted by selected jurisdictions in managing UCEM, with reference to Canada, Australia, Singapore, and the European Union. In formulating the proposed policy framework under the newly introduced Section 233A of the CMA 1998, the Commission has reviewed these international models to ensure that Malaysia's approach is practical, effective, and aligned with internationally recognised standards.

A common feature across most international regulatory regimes addressing spam is the use of a consent-based model. Canada's Anti-Spam Legislation ("**CASL**") requires prior (express or implied) consent before a commercial electronic message may be sent. The European Union's ePrivacy Directive similarly mandates an opt-in requirement for direct marketing via electronic mail and automated calling systems. Australia's Spam Act 2003 recognises both express and inferred consent. In contrast, Singapore's Spam Control Act 2007 adopts an opt-out model, where unsolicited commercial messages are permitted, provided they include a functional unsubscribe mechanism.

Sender identification and message labelling requirements are another consistent regulatory element. Both Australia and Singapore require commercial messages to clearly state the identity and contact information of the sender. Singapore mandates the inclusion of specific labels (e.g. "<ADV>") in the subject line of unsolicited messages to indicate their promotional nature.

Unsubscribe mechanisms are regarded as critical safeguards. All four jurisdictions require commercial messages to include a cost-free, simple means for recipients to opt out of future communications. These mechanisms must remain operational for a specified period and unsubscribe requests must typically be processed within five to ten working days, depending on the jurisdiction.

Canada and Australia also prohibit the acquisition or use of address harvesting software and lists generated through automated or deceptive means. Under CASL and Australia's Spam Regulations, it is an offence to acquire, use, or distribute such tools or data. These provisions aim to deter bulk, non-consensual messaging practices that exploit user data.

Jurisdictional reach is an increasingly important consideration. Canada's CASL applies to any message accessed in Canada, regardless of where it originates. The European Union framework, under Article 3(2) of the General Data Protection Regulation ("**GDPR**"), applies to senders who target EU residents or monitor their behaviour. Australia applies an "Australian link" test, encompassing messages sent to, from, or via infrastructure located in Australia. Singapore's regime similarly applies to messages sent from or accessed within its territory.

Malaysia's proposed Regulatory Framework for UCEM draws from these international best practices. It integrates key regulatory safeguards such as consent models, unsubscribe rights, sender transparency, and prohibitions on harvesting, while tailoring their implementation to reflect local enforcement capacities, legal constructs, and user context. In doing so, the framework aims to strike a balance between enhancing consumer protection and supporting responsible digital marketing in Malaysia's evolving digital economy.

## **2.1 Key Definitions**

### **2.1.1 Definition of Unsolicited Commercial Electronic Messages**

“Unsolicited Commercial Electronic Messages” (“**UCEM**”) refers to any commercial electronic message sent through any communication mode, where there is no prior relationship between the sender and the recipient, or no prior consent from the recipient.

### **2.1.2 Definition of Electronic Message**

“Electronic message” means any message sent using a network service or applications service to an electronic address, endpoint, or similar communication mode, regardless of whether the address exists or whether the message reaches its intended recipient.

### **2.1.3 Definition of Commercial Electronic Message**

“Commercial Electronic Message” means any electronic message sent by electronic means for the purpose of promoting, offering, marketing, or supplying:

- a) products or services;
- b) land or any interest in land;
- c) business or investment opportunities; or
- d) a person or entity that provides such products, services, or opportunities

This includes messages that:

- a) contain direct or indirect promotional content;
- b) request consent to send future commercial content;
- c) include links, contact details, or embedded features intended to lead the recipient to a commercial engagement,
- d) are sent via, including but not limited to, e-mail, SMS, internet messaging services, or similar communication modes.

This definition excludes messages sent by public authorities or government-designated entities for purposes related to law enforcement, public safety, emergency services, national security, or official government communications.

#### **2.1.4 Definition of Sender and Recipient**

- a) "Sender" means any individual, organisation, or entity that sends, authorises the sending of, or causes the sending of a commercial electronic message, whether directly or indirectly, through any telecommunications service, system, or platform, including by means of automated or delegated transmission technologies.
  
- b) "Recipient" means any individual, organisation, or entity who is the account holder of the electronic address or endpoint to which a commercial electronic message is sent. This includes any other person who uses, is intended to use, or is capable of accessing that electronic address, including shared, group, or dynamically assigned addresses.

#### **2.1.5 Definition of Address Harvesting and Dictionary Attacks**

- a) "Address harvesting" means the automated collection of electronic addresses (such as email addresses or phone numbers) from websites, databases, or online sources without consent, typically for the purpose of compiling bulk messaging or spam list.
  
- b) "Dictionary attack" means a method in which senders or attackers systematically generate and test common address combinations (e.g., user123@example.com) in an attempt to identify valid addresses, often for use in spam distribution or account intrusion.

## **SECTION 3: CORE ELEMENTS OF UCEM**

### **3.0 Malaysian Link**

For the purpose of establishing jurisdiction, a commercial electronic message is considered to have a Malaysian link in accordance with the territorial and extra-territorial application under Section 4 of the CMA 1998.

A commercial electronic message is deemed to have a Malaysian link if any of the following conditions apply:

a) Sender-based connection

The individual or organisation that sends, causes to be sent, or authorises the sending of the message is:

- Physically present in Malaysia at the time the message is sent; or
- An individual who is a Malaysian citizen or permanent resident, regardless of physical location; or
- An organisation formed, incorporated, or carrying on business in Malaysia, regardless of where the message is sent or the infrastructure used.

b) Recipient-based connection

The message is addressed to, or accessed by:

- An individual physically present in Malaysia;
- A Malaysian citizen or permanent resident, regardless of current location; or
- An organisation that is formed, incorporated, or operating in Malaysia.

c) Infrastructure-based connection

The message is accessed through a computer, server, device, or telecommunications network infrastructure located in Malaysia.

d) Intent-based connection or undeliverable message

A message that cannot be delivered due to a non-existent address may still be linked to Malaysia if there is evidence of intent to target Malaysian users.

This includes cases where:

- the electronic address used is associated with Malaysia (e.g. domain ending in “.my”); or
- the content of the message suggests it was reasonably intended for access by a person or infrastructure in Malaysia, based on factors such as language, currency, geographic references, or other identifiable targeting indicators.

### **3.1 Prohibition of Address Harvesting and Dictionary Attacks**

a) Prohibited tools and practices

No person should acquire, distribute, make available, or use any of the following for purposes related to the sending of unsolicited commercial electronic messages:

- Automated tools or software designed to extract electronic addresses from online sources;
- Software or mechanisms that generate addresses through automated or pattern-based guessing (commonly referred to as “dictionary attacks”);
- Any database or list of electronic addresses obtained through such means; or
- The rights to access, sell, or use such software or harvested lists, including where obtained indirectly.

b) Prohibition on sending to harvested or generated addresses

Senders should not initiate or authorise the sending of unsolicited commercial electronic messages to any electronic address that:

- was obtained using address-harvesting software or compiled through a harvested list; or
- was generated through dictionary attacks or similar automated guessing techniques.

### **3.2 Consent**

For the purposes of this framework, “consent” refers to a voluntary, specific, informed, and unambiguous indication of the recipient’s agreement to receive commercial electronic messages, provided either:

- a) expressly, through a clear, affirmative act by the recipient; or
- b) impliedly, inferred from the recipient’s conduct, business activities, or existing relationship with the sender.

#### **3.2.1 Types of Consent**

- a) “Express consent” refers to consent that is clearly and affirmatively given by the recipient. It is typically obtained through deliberate means such as checking an unchecked box, submitting a form, or providing written or electronic confirmation. Express consent must be explicit and cannot be assumed through silence or inactivity.
- b) “Implied consent” refers to consent that may be reasonably inferred from the existence of a prior or ongoing relationship between the sender and the recipient. This includes commercial or transactional relationships, such as the purchase of goods or services, membership or subscription arrangements, or other interactions that would reasonably create expectations of receiving related communications.

### 3.2.2 Requirements for Express Consent

For consent to be considered valid under the proposed framework, express consent must meet the following criteria:

a) Voluntariness

Consent must be given freely by the recipient, without coercion, deception, or undue pressure.

b) Specificity

Consent must be limited to the specific purpose of receiving commercial electronic messages. It should not be bundled with other terms or conditions unrelated to such communications.

c) Transparency

At the time of obtaining consent, the recipient must be clearly informed of the sender's identity, the purpose(s) for which the messages will be sent, and the types or categories of messages to be expected.

d) Revocability

Recipients must be able to withdraw their consent at any time through a free, accessible, and functional opt out mechanism. The withdrawal must take effect within a reasonable timeframe, and in any case not later than 10 working days from the date of the request.

e) Record-Keeping

Senders must retain verifiable records of how, when, and by whom consent was obtained. These records must be retained as long as necessary to demonstrate compliance and facilitate enforcement or dispute resolution, in line with applicable data protection obligations under the Personal Data Protection Act 2010 ("**PDPA 2010**").

### 3.2.3 Requirements for Implied Consent

Implied consent may be relied upon in limited circumstances where it is reasonable to expect that the recipient may receive commercial communications, based on prior relationship. The use of implied consent must satisfy all the following conditions:

#### a) Established Relationship

There is a prior or existing relationship between the sender and the recipient, such as:

- A commercial transaction involving the purchase, lease, or use of goods or services;
- A membership, subscription, or account relationships; or

Other business or non-commercial interactions that reasonably give rise to an expectation of receiving related communications.

#### b) Relevance of Content

The content of the commercial electronic message must be directly related to the nature of the existing or prior relationship. Promotional or marketing content should pertain to goods, services, or matters that are similar to, or reasonably connected with, those involved in the relationship.

#### c) Time Limitation<sup>5</sup>

Implied consent is valid only for a limited period from the last date of interaction:

- Up to 24 months from the date of the last transaction or engagement; or
- Up to 6 months from the date of an enquiry or application, where no subsequent transaction occurred.

---

<sup>5</sup> These timeframes are proposed as reasonable thresholds to reflect when a recipient may still reasonably expect to receive communications and are intended to complement the general principles under the PDPA 2010.

d) Revocability

Recipients must be provided with a clear, accessible, and functional mechanism to opt out at any time. Once the recipient has opted out, no further commercial electronic messages may be sent to that address.

e) Record-Keeping

Senders must maintain reasonable records demonstrating the existence of the prior relationship or transaction from which implied consent was derived. These records should be retained only as long as necessary for compliance verification or investigation, in accordance with the retention principles of the PDPA 2010.

### **3.3 Mandatory Message Requirements**

All commercial electronic messages must include specific information to support transparency, recipient awareness, and responsible communication practices.

#### **3.3.1 Clear Sender Identification**

Every commercial electronic message must clearly identify the sender and provide valid, accurate, and accessible contact details that allows the recipient to make enquiries, submit complaints, or withdraw consent.

The key elements of this requirement are:

a) Clear Identification:

The name or legally registered business identity of the sender must be clearly displayed within the body of the message.

b) Valid Contact Information:

The message must provide functional and responsive contact details (such as email address, phone number, or link to a contact form) that the recipient can easily use.

c) Accessibility:

Contact channels must be readily accessible and free of unnecessary barriers. This includes avoiding login requirements, obscure navigation, or broken links.

d) Accuracy and Maintenance:

The contact information provided must remain accurate and functional for a reasonable period following the sending of the message. A minimum duration of 30 calendar days is recommended.

### **3.3.2 Functional Opt-Out Facility**

All commercial electronic messages must include a clear, functional, and no-cost mechanism for recipients to withdraw their consent and unsubscribe from receiving further communications. The opt-out facility should meet the following criteria:

- a) Recipients must not be charged, required to log in, or made to complete lengthy forms to opt out.
- b) The mechanisms for unsubscribing must be user-friendly, easily accessible, and efficient.
- c) The opt-out mechanism must remain operational for at least 30 calendar days after the message is sent.
- d) All opt-out requests must be processed within 5 business days.

### **3.3.3 Accurate Message Labelling**

All commercial electronic messages must be clearly and accurately labelled to ensure transparency and prevent misleading or deceptive practices. The following elements apply:

a) Subject Field Clarity

Where a subject field is present, it must include a title that accurately reflects the content of the message. The subject line must not be false, misleading, or deceptive in any manner.

b) Advertisement Identifier

The letters "<ADV>", followed by a space, must appear at the beginning of the subject line to indicate that the message is an advertisement. If the message does not contain a subject line, the "<ADV>" tag must appear within the first line of the message body.

c) Header Integrity

The message must include header information (such as sender name, reply-to address, and routing data) that is not false, misleading, or deceptive in any respect.

d) Sender Contact Information

The message must include an accurate and functional electronic address or telephone number through which the sender can be readily contacted for enquiries, clarifications, or opt-out requests.

## **SECTION 4: SUBMISSION OF RESPONSES**

The Commission welcomes written submissions on any aspect of this Public Consultation document. All submissions must be submitted in full no later than **5:00 PM, 27 August 2025 (Wednesday)**.

Stakeholders may request confidential treatment for any part of their submission that is considered proprietary, commercially sensitive, or otherwise confidential. Such requests must include clear justification and will be subject to the Commission's review.

Where confidentiality is requested, respondents must also submit a corresponding non-confidential version of the submission. All confidential information should be redacted and placed in a separate annex clearly marked as "**CONFIDENTIAL**."

If a request for confidential treatment is granted, the relevant material will be reviewed by the Commission but will not be published. However, the Commission will not accept any submission in which confidentiality is claimed over the entire document or a substantial portion thereof.

Written submissions on this matter may be provided to the Commission in either hard copy or electronic form at the following:

**Address:**

The Chairman

Malaysian Communications and Multimedia Commission

MCMC HQ Tower 1, Jalan Impact, Cyber 6, 63000 Cyberjaya,

Selangor Darul Ehsan

(Attention: Regulatory Policy Division)

**Email:**

[policy.research@mcmc.gov.my](mailto:policy.research@mcmc.gov.my)

## ANNEX I: Template For Response

The Commission invites stakeholders to provide written feedback using the format below. Clear, concise responses with justification or supporting evidence are highly encouraged.

Components	Feedback
2.2.1 Definition of UCEM	
2.2.2 Definition of Electronic Message	
2.2.3 Definition of Commercial Electronic Message	
2.2.4 Definition of Sender and Recipient	
2.2.5 Definition of Address Harvesting and Dictionary Attacks	
3.1 Malaysian Link	
3.2 Prohibition of Address Harvesting and Dictionary Attacks	
3.3 Consent	
3.3.1 Definition of Type of Consent	
3.3.2 Requirement for Express Consent	
3.3.3 Requirement for Implied Consent	
3.4 Mandatory Message Requirements	
3.4.1 Clear sender identification	
3.4.2 Functional opt out facility	
3.4.3 Accurate message labelling	