TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION

Public Consultation Paper Issued on Proposed Regulatory Framework for Retention, Preservation and Disclosure of Communications Data for Investigation Purposes

Introduction

Following the recent amendments to the Communications and Multimedia Act 1998 ("**CMA**"), in particular the introduction of:

1. sections 252A and 252B in respect of preservation of communications data (which have yet to come into force); and

2. sections 268A in respect of the Minister's powers to prescribe rules on the retention of communications data to facilitate investigation of offences (which came into force in February 2025),

the Malaysian Communications and Multimedia Commission ("**MCMC**") recently issued a public consultation paper to gather views from key stakeholders on the Proposed Regulatory Framework on Retention, Preservation and Disclosure of Communications Data for Investigation Purposes ("**Proposed Regulatory Framework**").

The Proposed Regulatory Framework aims to enhance law enforcement agencies' investigative capabilities, and provide clear legal and operational guidance for service providers while protecting individual privacy through defined safeguards and due process.

This Update provides an overview of the key elements addressed in the Proposed Regulatory Framework, offering insights into what can be expected in the forthcoming regulatory framework once finalised, as well as the potential implications on stakeholders in Malaysia's communications and multimedia industry. The public consultation period for the Proposed Regulatory Framework is open until **8 August 2025**, and the online feedback form is accessible here.

Overview of the Guidance and Requirements in the Proposed Regulatory Framework

The Proposed Regulatory Framework sets out the following key elements:

Areas	Proposed Requirements
Scope	The Proposed Regulatory Framework will be applicable to: 1. all licensees under the CMA (i.e. Applications Service Providers (ASP), Content Applications Service Providers (CASP), Network Facilities Providers (NFP) and Network Service Providers (NSP)), that will be responsible for the provision, operation, or support of the communications systems and services that generate or store communications data; and 2. non-licensees that exercise control over a communications system including the system's infrastructure, or platform that facilitates the transmission, storage, or exchange of communications which may contain the communications data relevant for investigation purposes. These would include, but is not limited, to the following: • entities not licensed under the CMA, such as technology vendors, equipment providers, or platform operators whose communications systems form an integral part of the communications chain; and • relevant vendors that operate or manage network infrastructure containing communications systems, or that operate or manage communications platforms on behalf of the licensees (collectively, "**Entities**").
Definitions	For the purposes of the Proposed Regulatory Framework, the following definitions shall apply: 1. adopting the same definition under section 6 of the CMA, "**Communications data**" means any data relating to: • a communication by means of a communications system, generated by the communications system that formed a part in the chain of communications, indicating amongst others, the origin, destination, geolocation, route, time, date, size, duration or type of underlying service, of the communication;

Areas	Proposed Requirements
	• a subscriber of communications services and use of the communications services and the related products, services and applications by the subscriber; and • other data relating to communication. 2. "**Data Retention**" means the proactive obligation of retaining or storing specified communications data by entities (in this case, the Entities) for a specified period for the purpose of investigations. 3. "**Data Preservation**" means the act to preserve specified communications data by entities (i.e. the Entities) for a specified period, pursuant to a written notice from an authorised officer or police officer for the purpose of investigations. 4. "**Data Disclosure**" means the act of making available and disclosing stored and specified communications data by entities (i.e. the Entities), pursuant to a written notice from an authorised officer or police officer for the purpose of investigations.
Categories and Types of Communications Data Subject to Retention	For the purpose of the Proposed Regulatory Framework, "*communications data*" refers specifically to metadata generated by communications systems, excluding the actual content of the communications. This would include (but is not limited to) time or location of calls, subscriber and registration details, communication equipment information, technical identifiers and records of service of feature usage. All relevant Entities are required to retain the applicable categories and types of communications data as follows: 1. subscriber and end-user information; 2. service registration information; 3. technical identifiers; 4. location information; 5. communications metadata; and 6. temporal markers. However, this obligation is intended to be applied proportionately as not all entities may generate, store or access every type of communications data specified above.

Areas	Proposed Requirements
Retention Period for Communications Data	The relevant Entities are required to retain communications data for a minimum period of **12 to 18 months** for investigation purposes. Entities are allowed to retain communications data for a period longer than the minimum requirement.
Data Preservation Mechanism	Data preservation may be initiated upon a formal written request by an authorised officer or police officer, through a document referred to as a "**Preservation Notice**". This notice will be issued based on a reasonable belief that the data is relevant and required for an investigation. The standard period for data preservation is proposed to be **90 days**, which may be extended, where necessary, until investigation is completed. The contents of a Preservation Notice may include, but is not limited to, the following details: 1. the identity of the person in control of the communications system to whom the notice is directed; 2. a clear description of the communications data to be preserved; 3. the specific period for which the data is to be preserved; 4. instructions on the manner of preservation; and 5. any additional requirements or restrictions that shall apply. All Preservation Notices will be treated as confidential and any information relating to them will not be disclosed, except where required for civil or criminal proceedings under written law. Any Entities subject to a Preservation Notice will be required to maintain proper records of all preservation activities, which include: 1. the identity of the authority that requested preservation; and 2. a description of the communications data preserved.
Data Disclosure Mechanism	Access to stored communications data for investigation purposes may be granted through a Disclosure Notice issued by an authorised office or police officer, in accordance with applicable laws and guided by the principles of necessity, proportionality, and legality. Such disclosure is permitted only where it relates to the investigation of offences as defined under the CMA and its subsidiary legislations. Each Disclosure Notice may include, but is not limited to, the following details:

Areas	Proposed Requirements
	1. the identity of the person in control of the communications system to whom the notice is directed; 2. a clear description of the communications data to be disclosed; 3. instructions on the manner of disclosure; and 4. any additional requirements or restrictions that may apply. All Entities involved in data disclosure will implement suitable technical and organisational safeguards to ensure secure storage, processing and transmission of disclosed data. These may include: 1. strict access controls to ensure only authorised personnel can handle the data; 2. encryption of data in storage and during transmission, where applicable; and 3. activity logging, monitoring systems, and breach reporting mechanisms. Entities shall also adhere to the Disclosure Principle in section 8 of the Personal Data Protection Act 2010, which requires that personal data be disclosed only for purposes directly related to the activity for which the data was collected, and only to parties who are legally authorised to receive such data. All Disclosure Notices are strictly confidential, except where required for civil or criminal proceedings under written law, to preserve the integrity of investigations and reducing the risk of compromising the disclosed data or subject of investigations.
Implementation Timeline	A phased approach will be adopted to implement the Proposed Regulatory Framework. The implementation timeline will consider varying level of readiness among the Entities, technical complexity of compliance and operational capacity to adapt to the new regulatory requirements. Following the finalisation and gazettement of the subsidiary legislation, a grace period of **six to 12 months** is proposed for implementation.

Comment

The public consultation paper provides valuable insights into the upcoming subsidiary legislation on retention, preservation and disclosure of communications data for investigation purposes.

In an era where cybercrimes are prevalent, the proposals set out in the Proposed Regulatory Framework reflect MCMC's efforts in harmonising practices and requirements for data retention,

preservation and disclosure across the Entities, to ensure efficient access to to communications data, while upholding robust safeguards for security, accountability, and privacy. These efforts are aligned with Malaysia's broader legislative and international cooperation initiatives, including the plan to accede to the Budapest Convention on Cybercrime 2001 and to sign the new United Nations Convention on Cybercrime in October this year, both of which are aimed at strengthening international cooperation strategies in investigations, information sharing, and the exchange of digital evidence to combat cybercrimes.

We encourage stakeholders in the communications and multimedia industry to review the consultation paper and assess how the proposed requirements may affect their data governance and operational procedures. Stakeholders are also encouraged to provide feedback, particularly regarding any concerns about the practicality or potential challenges in implementing the proposed requirements. Additionally, if any further clarification is needed on specific aspects addressed in the public consultation paper, such issues should be clearly highlighted in the feedback.

The finalisation and implementation of this regulatory framework will undoubtedly have direct implications on the Entities, particularly in relation to their data governance practices. Thus, all Entities are advised to be monitor and stay updated with these developments and to prepare accordingly.

We trust the above provides a helpful overview of the guidance/key requirements proposed by the public consultation paper. Should you require any assistance or clarification regarding the above or any other matter relating to technology, media and telcommunications (TMT) and data protection, please feel free to get in touch with us at your convenience.

Contacts

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION

Deepak Pillai

HEAD

D +60 3 2275 2675
F +60 3 2273 8310
deepak.pillai@christopherleeong.com

Kuok Yew Chen

PARTNER

D +60 3 2267 2699
F +60 3 2273 8310
yew.chen.kuok@christopherleeong.com Intan

Haryati Binti Mohd Zulkifli

PARTNER

D +60 3 2675 2674
F +60 3 2273 8310
intan.haryati@christopherleeong.com

Yong Shih Han

PARTNER

D +60 3 2273 1919
F +60 3 2273 8310
shih.han.yong@christopherleeong.com

Anissa Maria Anis

PARTNER

D +60 3 2267 2750
F +60 3 2273 8310
anissa.anis@christopherleeong.com

Tiew Kai Xiang

PARTNER

D +60 3 2273 1919
F +60 3 2273 8310
kai.xiang.tiew@christopherleeong.com

Contribution Note

This Legal Update is contributed by the Contact Partners listed above, with the assistance of **Joy Lee** (Associate, Christopher & Lee Ong) and **Leslie Bong** (Pupil-in-Chambers, Christopher & Lee Ong).

Please feel free to also contact Knowledge Management at RTApublications@rajahtann.com.

Regional Contacts

Cambodia

Rajah & Tann Sok & Heng Law Office

T +855 23 963 112 | +855 23 963 113
kh.rajahtannasia.com

China

Rajah & Tann Singapore LLP Representative Offices

Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820

Shenzhen Representative Office
T +86 755 8898 0230
cn.rajahtannasia.com

Indonesia

Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

Lao PDR

Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

Malaysia

Christopher & Lee Ong

T +603 2273 1919
F +603 2273 8310
www.christopherleeong.com

Myanmar

Rajah & Tann Myanmar Company Limited

T +951 9253750
mm.rajahtannasia.com

Philippines

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)

T +632 8248 5250
www.cagatlaw.com

Singapore

Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand

Rajah & Tann (Thailand) Limited

T +66 2656 1991
F +66 2656 0833
th.rajahtannasia.com

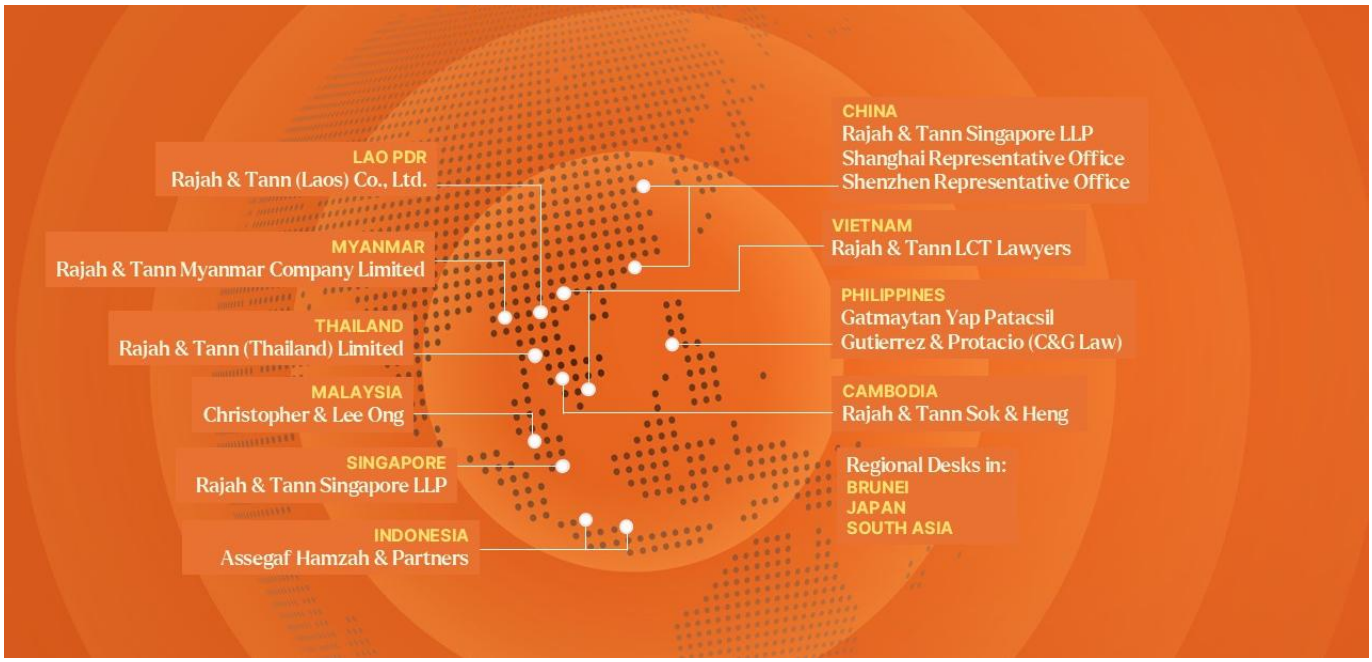
Vietnam

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127 | +84 24 3267 6128
vn.rajahtannasia.com

Our Regional Presence



Christopher & Lee Ong is a full service Malaysian law firm with offices in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of Christopher & Lee Ong, who are Malaysian-qualified, have accumulated considerable experience over the years in the Malaysian market. They have a profound understanding of the local business culture and the legal system and are able to provide clients with an insightful and dynamic brand of legal advice.

Christopher & Lee Ong is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.