Technology, Media & Telecommunications

Licensing Framework for Cybersecurity Service Providers Comes into Operation

Introduction

The Cybersecurity Agency of Singapore ("**CSA**") has announced the launch of the licensing framework for cybersecurity providers ("**Framework**"), which has taken effect from 11 April 2022. The Framework imposes a licensing requirement for the provision of prescribed cybersecurity services and sets out a series of licensing requirements and conditions.

The Framework aims to better safeguard consumers' interests and address the information asymmetry between consumers and cybersecurity service providers. It also seeks to improve service providers' standards and standing over time.

CSA had earlier conducted an industry consultation on the proposed Framework in September 2021. Our Legal Update on the Industry Consultation Paper on the Licensing Framework for Cybersecurity Service Providers is available here. CSA has since published details on the feedback received and the resulting key revisions made to the Framework in its industry consultation closing note, available here.

The Framework has been enacted via Part 5 and the Second Schedule of the Cybersecurity Act, which came into operation on 11 April 2022. Subsidiary legislation such as the Cybersecurity (Cybersecurity Service Providers) Regulations 2022 has also been enacted as part of the Framework.

The enacted Framework contains certain amendments from the version proposed in the industry consultation. This Update provides an updated summary of the key elements of the Framework, including the scope of licensing, the licensing requirements and the licence conditions, as well as the timeline for compliance.

Timeline

CSA has set out the timeline for the relevant cybersecurity service providers to comply with the licensing requirements of the Framework:

- **11 April 2022** – No person may provide a licensable cybersecurity service without a cybersecurity service provider's licence from 11 April 2022. CSA has provided a six-month grace period for those already engaged in the businesses of providing licensable cybersecurity services as at this date.

- **11 October 2022** – Existing cybersecurity service providers who are already engaged in the businesses of providing licensable cybersecurity services must apply for a licence by 11 October 2022. If the licence application is made by 11 October 2022, the service provider may continue to provide its service until a decision on its application has been made.

  Any person who engages in the business of providing any licensable cybersecurity services without a licence after 11 October 2022 shall be liable to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding two years or to both.

- **11 April 2023** – If a licence application is lodged within the first 12 months (by 11 April 2023), there will be a one-time 50% waiver of the licence fees so as to support businesses due to the impact of COVID-19. Otherwise, the licence fees for individuals and businesses are S$500 and S$1,000 respectively.

The licence is valid for a period of two years, and an application for renewal should be made no later than two months before the expiry of the licence.

Scope of Licensable Services

For a start, CSA will license two types of cybersecurity service providers:

(a) **Managed security operations centre monitoring services** – a service for the monitoring of the level of cybersecurity of a computer or computer system of another person by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system.

(b) **Penetration testing services** – a service for assessing, testing or evaluating the level of cybersecurity of a computer or computer system, by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system.

These services have been prioritised because service providers can have significant access into their clients' computer systems and sensitive information. Further, these services are already widely available and adopted in the market, and thus have the potential to cause significant impact on the overall cybersecurity landscape.

CSA has reiterated that all cybersecurity service providers that provide either or both of these licensable cybersecurity services to the Singapore market will need to obtain separate licences for each service. This includes:

(a) Companies or individuals (i.e. freelancers or sole proprietorships owned and controlled by individuals) who are directly engaged in such services;

(b) Third-party cybersecurity service providers that provide these services in support of other cybersecurity service providers; and

(c) Resellers or overseas cybersecurity service providers who provide licensable cybersecurity services to the Singapore market.

CSA has stated that it will not exclude re-sellers or sub-contractors from licensing requirements, and that so long as any such entities engage in the business of providing any licensable cybersecurity service to the Singapore market, they must be licensed. CSA has clarified that where a cybersecurity service provider partners with or leverages the resources of an affiliate entity from its corporate group (which may be local or overseas) to provide licensable cybersecurity services, every entity within the corporate group involved in the provision of licensable cybersecurity services to the same client(s) would be required to take up a licence. Regardless of the type of legal arrangement entered into, the Framework seeks to ensure that all such persons are fit and proper. In this regard, requiring only one entity in the corporate group or one link in the reselling chain to be licensed would undermine the regulatory objective of the Framework.

Key Conditions of the Licensing Framework

Application for licence

An application for the grant or renewal a licence must be made electronically at https://www.gobusiness.gov.sg/licences.

The following information must be provided in an application:

(a) Prescribed information on the applicant's identity;

(b) Information on the qualification or experience of the applicant (for individuals) or key officers (for business entities) relating to the licensable cybersecurity service for which a licence is sought;

(c) Where the information in (b) is not available, information on the applicant's employees having supervisory responsibility relating to the licensable service; and

(d) Information on whether the applicant is fit and proper (e.g. compoundable offences involving fraud, dishonesty or moral turpitude, bankruptcy or insolvency status, previous revocation of licence).

Keeping of records

The Framework imposes a record-keeping requirement on licensees. For each occasion the licensee is engaged to provide its cybersecurity service, the licensee must keep record of the following information for a period of at least three years:

(a) The name and address of the person engaging the licensee for the service;

(b) The name and individually identifiable information of the person providing the service on behalf of the licensee – for individuals, this would be the name and the unique identification number of the individual; for companies, this would be the business entity's name and unique entity number;

(c) The date on which the service is provided; and

(d) Details on the type of service provided.

If a licensee furnishes a false or misleading record, the licensee shall be liable to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding 12 months or to both.

Notification on changes to information

To ensure that the licensees' key officers are fit and proper, licensees are to notify the licensing officer within 14 days after the appointment of new key officer(s). Licensees must also notify the licensing officer of any change in or inaccuracy of the information and particulars that the licensee had previously submitted within 14 days upon occurrence of the event. Such events include situations such as key officers ceasing to hold office, changes to the licensee's and/or its key officer's address and contact particulars, or criminal convictions entered against the licensee and/or its key officers.

Professional conduct of licensee

To provide a baseline level of protection for consumers of cybersecurity services, licensees will be required to comply with certain requirements on professional conduct such as the following:

(a) Not make any false representation in the course of advertising or providing its cybersecurity service;

(b) Comply with all applicable laws in the course of providing its cybersecurity service, including, but not limited to, the Computer Misuse Act and all obligations relating to confidentiality and data protection;

(c) Exercise due care and skill, and act with honesty and integrity in the course of providing its cybersecurity service;

(d) Not act in a manner where there is a conflict between its interests and that of the person procuring or receiving the cybersecurity service; and

(e) Collect, use, or disclose any information relating to the person procuring or receiving the licensable cybersecurity service only for the purposes of providing such service.

Provision of information to the licensing officer

Licensees are required to provide the licensing officer with information concerning such matters that relate to their cybersecurity service upon request.

In light of feedback suggesting that the language of this condition be tightened to avoid requests that are overly broad, CSA has indicated that it has revised the language of the conditions to reduce uncertainty for licensees. CSA has also indicated that any such information requested would be limited to what is necessary for the purpose of the investigation.

New Cybersecurity Services Regulation Office

CSA has set up the Cybersecurity Services Regulation Office ("**CSRO**") to administer the Framework and facilitate liaisons with the industry and wider public on all licensing-related matters. The functions of the CSRO include:

(a) Enforcing the licensing framework;

(b) Responding to queries and feedback from licensees, businesses and public; and

(c) Developing and sharing resources on licensable cybersecurity services with consumers such as the list of licensees.

Further information on the licensing framework and CSRO is available at https://www.csro.gov.sg.

Concluding Remarks

The licensing framework for cybersecurity service providers, the development of which has been closely watched by the cybersecurity industry, has come into operation after a period of consultation and feedback. Cybersecurity providers must now ensure that they comply with the licensing requirements, or else face potential fines and/or imprisonment should they be found guilty of an offence.

Cybersecurity providers should address the following issues relating to an application for a licence:

(a) Do the cybersecurity services offered fall within the prescribed list of licensable services?

(b) If they are an existing cybersecurity service provider, they should ensure that they meet the relevant timeline for applying for the licence.

(c) Applicants should ensure that they meet the criteria for application.

Cybersecurity providers should also be aware that, once licensed, they face a series of obligations relating to the keeping of records and professional conduct. Licensees should ensure that they have policies and procedures in place to comply with these obligations, and may wish to review their existing practices and operation to assess whether they meet the necessary standards.

For further queries, please feel free to contact our team below.

Contacts

Rajah & Tann Singapore LLP

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751
rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786
steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0738
benjamin.cheong@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications

T +65 6232 0752
lionel.tan@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade; Technology, Media & Telecommunications

T +65 6232 0298
tanya.tang@rajahtann.com

Rajah & Tann Technologies

Michael Lew
Chief Executive Officer, Rajah & Tann Technologies

T +65 6932 2609
michael.lew@rttechlaw.com

Rajah & Tann Cybersecurity

Wong Onn Chee
Chief Executive Officer, Rajah & Tann Cybersecurity

T +65 6932 2606
onnchee@rtcybersec.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *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

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

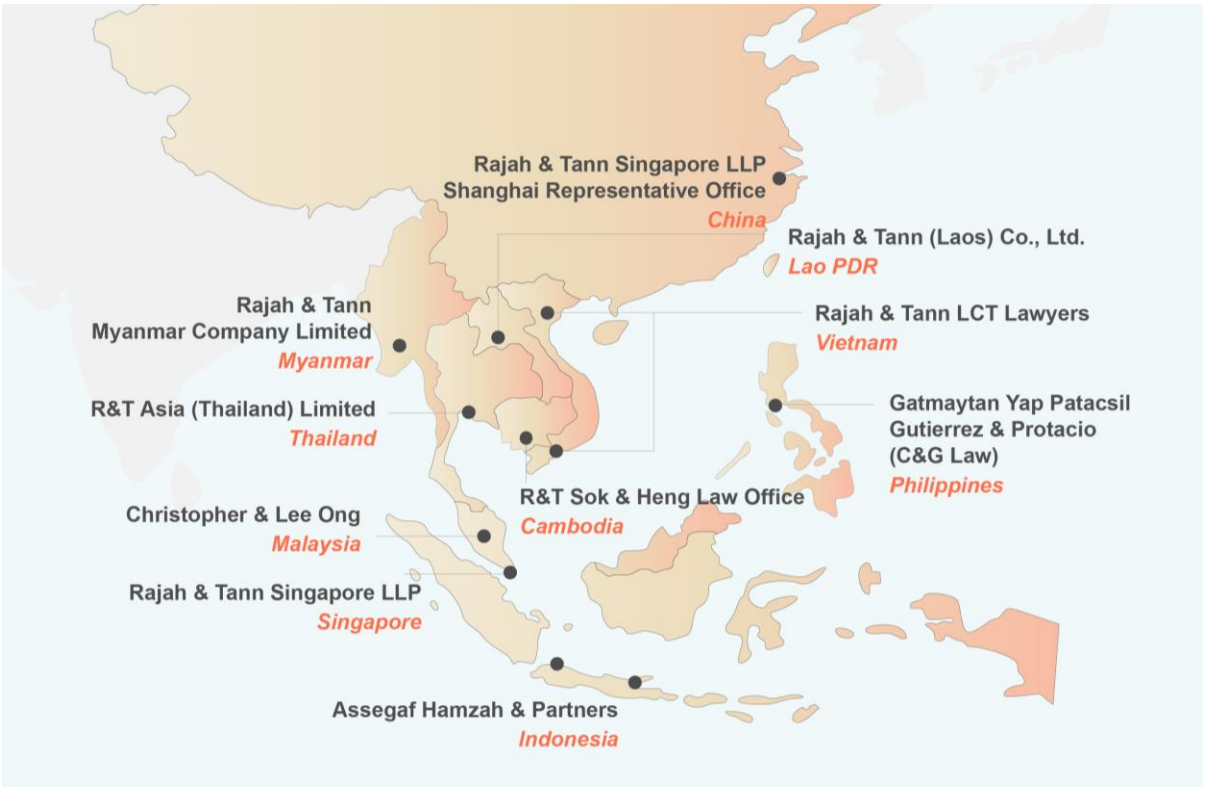
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP 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.