

PRIVACY  
RULES

# Singapore Digital Spaces: Upcoming Measures to Enhance Online Safety

ORION 

The Singapore government will introduce several measures to counter online crimes and ensure safe and secure digital spaces. This builds on the Online Safety (Miscellaneous Amendments) Act 2022 which came into force on 1 February 2023. Please see [Singapore Introduces New Online Safety Provisions to Tackle Online Egregious Content](#) for more details on the Online Safety Act.

## Online Crimes

The Ministry of Home Affairs (**MHA**) will introduce the Online Criminal Harms Act (**OCHA**) later in 2023. The OCHA will criminalise online content that is criminal in its own right or content which facilitates or abets crimes, including syndicated crimes such as scams, online incitement of mass public disorder, phishing and distribution of malware. The OCHA will empower the MHA to stop or remove online communications that facilitate crimes in the physical world (e.g., inciting violence), increase the scope of entities it can act against (e.g., cover mediums of online communication through which criminal activities could be conducted) and introduce upstream measures to detect and reduce scams (e.g., safeguards against inauthentic accounts).

## App Stores and Online Games

The Ministry of Communications and Information (**MCI**) will issue a new Code of Practice for App Stores (**Code**) after 12 to 18 months of development and industry consultation. The Code aims to regulate issues relating to App Store applications with harmful content, especially for children (e.g., content depicting explicit sexual activities or inciting violence). Like social media services, App Stores will be expected to have systems and processes in place to deal with harmful content.

While the risks of exposure to harmful content through online games will be reduced through the Code, the MCI notes that online games may still be accessed through platforms other than App Stores. Therefore, the MCI will study how to deal with this regulatory gap and explore measures such as a classification scheme to clarify the age-appropriateness of online games to help parents exercise better supervision over their children's gaming.

## Cybersecurity Review

The Cyber Security Agency of Singapore (**CSA**) announced last year that it embarked

on a review of the Cybersecurity Act 2018 (**CS Act**) to expand the scope of the regulatory framework. The CS Act currently focuses on the protection of Critical Information Infrastructure (**CII**) against cyberattacks, where CII includes computers or computer systems within essential sectors such as energy, water, banking and finance, healthcare, transport, infocomm, media, security and emergency services and government services.

In a recent update, the MCI announced that the CSA has identified cloud services and data centres as foundational digital infrastructure that needs to be better protected and thus is likely to be included in the expanded scope of the CS Act. The CSA is also examining how Singapore's entire cybersecurity ecosystem can be developed to adapt to increasing industry digitalisation (e.g., nurturing talent and promoting innovation and capability development).

## Personal Data Protection for Artificial Intelligence

The Personal Data Protection Commission plans to publish two Advisory Guidelines in 2023 to ensure the responsible development and deployment of artificial intelligence (**AI**):

- Advisory Guidelines on the Use of Personal Data in AI Systems. These will contain transparency and explainability standards (to allow customers to understand when and how AI is being used to process their personal data) and best practices on how the industry can use personal data to train, test and monitor AI systems.
- Advisory Guidelines on Children's Personal Data. These will set out clear, actionable standards for social media services and companies when dealing with children's personal data. Such measures include obtaining parental consent before collecting data from children under the age of 13 and implementing protective defaults (e.g., ensuring children's profiles are not made public).

## Key Takeaway

The Singapore government's online safety initiatives are focused on protecting vulnerable end-users, particularly children. Businesses that provide online services (e.g., online communication, applications, games, cloud, data centres or AI) should continue to keep abreast of the developments and comply with such requirements after the issuance of such measures.

## For More Information

OrionW regularly advises clients on technology and media matters. For more information about technology and media, or if you have questions about this article, please contact us at [info@orionw.com](mailto:info@orionw.com).

Disclaimer: This article is for general information only and does not constitute legal advice.



WINNIE CHANG  
MANAGING DIRECTOR  
AT  
ORIONW



WINNIE.CHANG@ORIONW.COM



+65 6909 7801

ORIONW

# CONTACT US

## PrivacyRules

### **American Headquarters:**

PrivacyRules, Ltd.  
151 West 4th Street  
Suite 200  
Cincinnati, OH 45202, USA

### **European Office:**

Via dei Della Robbia 112,  
50132, Firenze  
Italy (IT)

### **Email**

info@privacyrules.com

[www.privacyrules.com](http://www.privacyrules.com)

