



Data Privacy Detective Podcast – Episode 49 – Hong Kong: What Impact of the National Security Law?

Jul 31, 2020

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

On June 30, 2020 China enacted a National Security Law applicable in Hong Kong. The UK and USA governments reacted negatively, stoking fears that this could mean the end of the one-country-two systems concept. Front-page news abounds about the meaning, the reach and the political implications.

But what about business and normal life, about Hong Kong's role as a global financial and technology center? How does one understand the impact on data privacy? Does this mean a replacement of Hong Kong law or will it be Hong Kong business as usual? In this podcast [Pádraig Walsh](#) of Tanner De Witt Solicitors, a leading Hong Kong law firm, guides us.

The new National Security Law focuses on secession, subversion, terrorism and collusion with foreign or external forces. It does not replace the longstanding data privacy laws and precedents of Hong Kong, put in place before the July 1, 1997 UK/PRC change of sovereignty and augmented with modern changes more like the approach of Europe than of China itself.

The National Security Law should be viewed as having little impact on business life and does not replace Hong Kong's data privacy laws and system of regulation beyond the scope of the National Security Law. Hong Kong's data privacy approach aligns with European concepts, with existing and currently planned updates based on principles like GDPR. For example, Hong Kong does not require data localization, unlike the PRC's code that requires data localization and takes a restrictive and pro-government view about the flow of personal data across borders and the right of the PRC government to access personal data. Considering the European Court of Justice's July 16, 2020 Schrems II decision, Hong Kong's approach can be viewed as more flexible than that of the EU regarding cross-border data flows. By contrast, Hong Kong follows its free-trade tradition in not restricting data flows, while nonetheless ensuring

protection of personal data through disclosure, consent and other measures.

China benefits from Hong Kong's common law system and its relatively free flow of goods, services and currency as a major global commercial center, used by many businesses as a kind of two-way gate between north Asia and the rest of the world. Bottom line? No reason to view the National Security Law as disrupting the well developed and balanced approach to data privacy that Hong Kong developed over decades. The vast majority of data privacy matters will be addressed through the Hong Kong system, not China's code, with the caution that personal data affecting "national security" will be subject to the law applicable throughout China and now including Hong Kong. In this sense, the concerns of China are the same as those of every government – striking a balance between order and freedom. That balance will be struck differently in different countries. It need not upset the flow of business and commerce or defeat the protection of personal privacy beyond the scope of national security.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.