20 ESSEX STREET

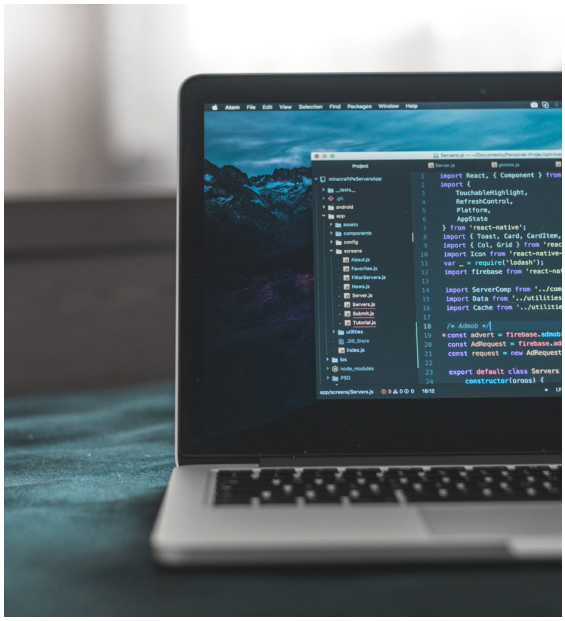
BULLETIN

March 2018

Disruptive Developments @20EssexStreet

Cybersecurity regulation post-Brexit: examples from Asia

Andrew Dinsmore



Cybersecurity protection in the United Kingdom will be composed of a patchwork of overlapping statutes and European Union regulations in the form of the Data Protection Act 1998 ("DPA"), the General Data Protection Regulation (679/2016/EU) (due to come into force on 25 May 2018, the "GDPR") and the Network and Information Security Directive (2016/1148/EU) (due to be implemented by 9 May 2018, the "NIS Directive").

There is an issue around the role of the GDPR and the implemented NIS Directive in the United Kingdom following Brexit.

The position in Singapore, Hong Kong and the People's Republic of China (PRC) are useful examples of different approaches to cybersecurity protection across Asia.

Singapore

Singapore has recently passed the Cybersecurity Act 2017, which is similar to the NIS Directive as it seeks to provide a framework for the regulation of 'critical information infrastructure'. This relates to those essential services listed in Sch. 1 including energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, Government and media. The Act also gives powers to the Cyber Security Agency of Singapore to investigate, and respond to, cybersecurity incidents alongside establishing a licencing regime for both investigative and non-investigative cybersecurity services provided by private entities.

Hong Kong

Hong Kong's position is governed by the Personal Data (Privacy) Ordinance which requires that organisations who collect, hold, process or use personal data must comply with its provisions as underpinned by six key principles:

1. Data collection
2. Accuracy and retention
3. Data use
4. Data security
5. Openness
6. Data access and correction

Compliance with the Ordinance is supervised by the Private Commissioner for Personal Data ("PCPD") and whilst Hong Kong has not yet introduced specific cybersecurity legislation comparable to the Singaporean Cybersecurity Act 2017, the PCPD has issued numerous guidelines which influence the PCPD when determining whether a private organisation is in breach of the Ordinance. Thus, these guidelines ensure that its provisions remain up-to-date and recent examples include guidelines on direct marketing, drones, technological innovation (including cookies, online tracking and behavioural advertising) and data breach handling.

PRC

The People's Republic of China brought into effect its Cybersecurity Law on 1 June 2017, which aims to protect personal information and individual privacy by standardising the collection and use of such data with the safeguarding of 'national cyberspace sovereignty' being a fundamental principle. To do so, the Cybersecurity Law seeks to

ensure greater protection of critical information infrastructure (which Art. 31 defines as public communications and information services, energy, finance, transportation, water conservation, public services and e-governance) through a framework of penalties to be imposed on 'network operators' including the suspension of business activities, the closure of business and revocation of licences (in the case of serious breaches) and the power to impose a fine up to the value of RMB1,000,000. The Cyberspace Administration of China, in conjunction with the Ministry of Public Security, supervises compliance with this regime.

Comment

The two key themes which emerge from these jurisdictions are:

1. There is a focus on cybersecurity threats to critical information infrastructure.
2. They seek to establish specific public institutions to regulate cybersecurity.

These two key themes also exist in the NIS Directive and it is hoped that the UK Government will view its implementation not as a necessity of EU Law but, rather, as a necessity of being a global economy and thus retain the implementing legislation, and the National Cyber Security Agency it seeks to establish, following Brexit.

For further information on the legal implications of cybersecurity breaches for financial institutions, see Andrew's recent article in the Journal of International Banking and Financial law; the citation for which is [2017] 11 JIBFL 676.

If you require advice on any of the topics discussed in this briefing from Andrew or any member of 20 Essex Street please contact: clerks@20essexst.com

Andrew Dinsmore

Andrew has a broad international commercial litigation and arbitration practice. He is often instructed to appear as junior counsel in complex, multi-jurisdictional, high-value cases and is also regularly instructed to appear as sole counsel in the Commercial Court, Chancery Division and in arbitration.

Andrew splits his time between London and Singapore. Read his online biography.

For further information about this bulletin contact: dking@20essexst.com

LONDON
20 Essex Street London WC2R 3AL
Tel +44 (0)20 7842 1200
Fax +44 (0)20 7842 6770

SINGAPORE
Maxwell Chambers, #02-09
32 Maxwell Road, Singapore 069115
Tel (+65) 62257230
Fax (+65) 62249462

clerks@20essexst.com