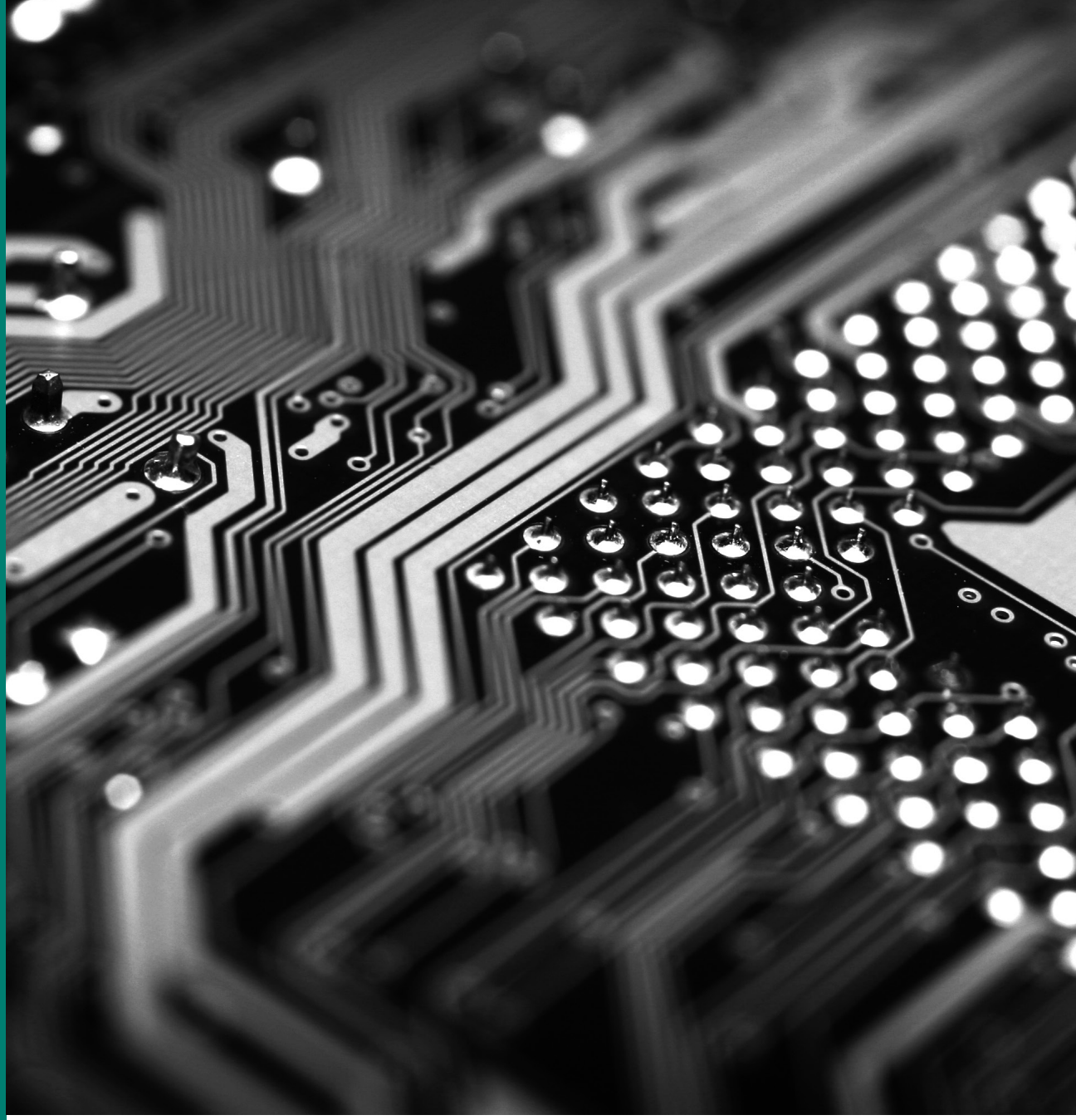
INSURANCE BULLETIN
OCTOBER 2018 EDITION 1



In this week's Insurance Bulletin:

Rupert Warren, Senior Associate, rupert.warren@hfw.com
Costas Frangeskides, Partner, costas.frangeskides@hfw.com

ROSIE NG
CONSULTANT

"The regulatory authorities retain the right to determine what constitutes "important data". This includes trade secrets, state secrets and other such information which the authorities consider sensitive. This is likely to include information which is political in nature."

1. REGULATION AND LEGISLATION

China: Cybersecurity Law and Data Localisation

On 1 June 2017, China's Cybersecurity Law (CSL) came into effect. This is the first comprehensive legislation of its kind providing a framework for data protection and governance of network and system security. The CSL applies to (i) Network operators, and (ii) Critical Information Infrastructure Operators.

Network operators

"Network operators" are defined as "owners, operators and service providers of networks". "Network" is deemed to be any system comprised of computers or other information terminals or equipment which are used for the gathering, storage, transmission, exchange and processing of information.

The CSL applies not only to businesses in China which manage their own data network but also companies based outside China who use networks to conduct business there.

Critical Information Infrastructure Operators (CIIO)

CIIO are entities which provide services which, if lost or destroyed, would seriously damage China's national security, economy or the public interest. The CSL provides examples of these, such as entities which operate in the public communications and information services, energy, transportation, water resources, finance and public services sectors.

Duties and obligations

The CSL imposes a number of key obligations on Network operators.

With regard to network systems, they are required to:

- Set up internal security and management systems and procedures, including the appointment of appropriate personnel to effect a secure network.
- Take technological measures to prevent viruses, combat cyber attacks and threats to network security (including monitoring the network activities carried out by their users).
- Keep a record of network activity and security breaches and to maintain this for a minimum of 6 months.
- Take security measures such as data classification, back-up systems and encryption.
- Set up a complaints reporting procedure.

With regard to personal data, they are required to:

- Seek and obtain consent from the relevant individual before collecting personal data; such data must pertain to the Network operators' services.
- Expressly set out the reason for, scope and method of collection and use of personal data.
- In the event of a data breach, make a report to the authorities, take necessary remedial steps and inform/notify the relevant affected individuals of the same.
- Review or amend personal data at the request of the relevant individual/user.

With regard to the monitoring of user content, they must:

- Monitor content published by the user.
- Report to the authorities and maintain records of illegal content.
- Remove illegal content.

CIIO are also subject to similar requirements.

Network operators are subject to "mandatory testing and certification". CIIO are also required to sign confidentiality and security agreements with their suppliers of network products and services and assess cybersecurity risks at least once a year.

Enforcement

Network operators and CIIO are required to cooperate fully with and provide access to the enforcement agencies when requested to do so.

The main enforcement authorities are:

- Cyberspace Administration of China (CAC) which has primary responsibility for the supervision and enforcement of the CSL.
- The Public Security Bureau (PSB) which has investigatory powers and enforces the CSL at local level.
- The Ministry of Industry and Information Technology which oversees the supervision and protection of personal data by telecom operators and internet information services.

The CAC and PSB are empowered to investigate matters and make the appropriate enforcement orders. There is no opportunity for Network operators or CIIO to make representations at a hearing. If they wish to appeal an order, they must do so through the Chinese Courts.

The majority of cases prosecuted to date by the CAC and the PSB relate to Network operators who have failed to properly manage the data of its users, failed to take necessary measures in protecting the relevant network, breached rules in the collection and use of personal data and the management of the user's identification.

Penalties/Orders

In the event of a breach, the following orders can be made by the enforcement authorities:

- Rectification (which has been the most common order to date)
- Suspension of business during the rectification
- Closure of website/apps or part of business
- Temporary removal of apps or cessation of new user sign up
- Imposition of penalty/fines
  - Individuals can be fined from: RMB5,000 (US$750) to RMB1,000,000 (US$150,000).
  - Breaches of the data localisation provisions (see below) may result in fines against companies of between RMB50,000 and RMB500,000 (US$7,500 - US$75,000).
- Detention
  - Network operators can be subject to five to fifteen days detention for breach of certain provisions.

More than one punitive measure can be taken against a Network operator or CIIO per enforcement action.

Civil claims have also been commenced under the CSL and there have been four published awards to date. These have arisen as a result of incorrect or false information posted online and/or a failure to verify the accuracy of the information on a website as well as the posting of defamatory information and/or graphic images relating to individuals. Damages have been awarded up to RMB40,000 (US$6,000)

Data localisation

On 31 December 2018, Article 37 of the CSL, relating to data localisation will come into effect. The basic requirement under Article 37 is that "personal information" and "important data" collected or produced by CIIO must be stored in China. This is a controversial provision which has been the subject of much criticism. In 2016, a joint statement signed by 40 international business groups sought an amendment to this provision but to no avail.

"Personal information" includes all information (whether in electronic form or otherwise) which individually or combined with other information allows the identification of a natural person. This includes personal information such as the name, date of birth, address, identity card number of the individual, etc. The regulatory authorities retain the right to determine what constitutes "important data". This includes trade secrets, state secrets and other such information which the authorities consider sensitive. This is likely to include information which is political in nature.

Subsequent draft rules and guidelines provide that Network operators will also be subject to the data localisation regime (as referred to below).

The draft Guidelines and Measures

The relevant draft rules and guidelines are:

- Draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (the Measures); and
- Draft Guidelines for Data Cross-Border Transfer Security Assessment (the Guidelines).

Both the Measures and the Guidelines apply to Network operators. The provisions also apply to overseas network providers (even if they do not have a presence or operation in China) who supply products or services to a client base in China. In these circumstances, the overseas Network operator would be considered to be engaged in domestic operation. Domestic operation, under the Guidelines, means one which provides products or services within China.

The Guidelines provide factors which are taken into account to determine whether a foreign company is engaged in domestic operation, such as the currency used for payments and the distribution of products to Chinese companies or Chinese nationals.

Consent

In order to transfer personal information outside China, the prior written or express consent by way of affirmation of the data subject must be obtained by the Network operator. (With regard to the latter, this could involve the simple "click" of a "Yes" or No" button online to denote approval or otherwise.) There are certain circumstances when consent is implied or deemed to have been given, for example, when sending an email internationally, when conducting international calls and when making a cross-border transaction over the internet. There is also an exemption which applies in the event of an emergency where there is a danger to the life or property of the data subject.

"Multi-national corporations who provide either services or products within China will need to store personal information and important data which has been collected or generated within China and will therefore need to comply with the new Measures and Guidelines."

Security assessments of data transfers

The Measures require that a self-assessment be conducted by a company which purports to transfer personal information or important data outside China. This will involve the preparation of a transmission plan which contains details of the data transfer. The plan is subject to a 'legal' and 'appropriateness' test. If this criteria is satisfied, the issue of whether the cross-border transfer is "controllable" is then addressed. Such assessment will be monitored by the Chinese regulatory authorities.

In addition to the self-assessment, there is also a second type of security assessment which is conducted by the regulated authorities where material data transfers are involved.

The key triggers for a security assessment by the regulatory authorities of a material data transfer include:

- The personal data relates to more than 500,000 data subjects.
- The size of the data to be exported exceeds 1,000GB.
- The data relates to large-scale engineering projects, defence/ military, public health, marine environmental, biochemical and nuclear sectors or involves sensitive geographical information.
- System vulnerabilities and security safeguards for critical information infrastructure or similar information.

Penalties/Orders

Penalties can be imposed upon the company and/or the directly responsible manager.

The fines can range from the following:

- Network operators: RMB50,000 to RMB500,000 (US$7,500 to US$75,000).

  The directly responsible manager: RMB10,000 to RMB100,000 (US$1,500 to US$15,000).

- CIIOs: RMB50,000 to RMB500,000 (US$7,500 to US$75,000).

  Directly responsible manager of CIIO: RMB10,000 to RMB100,000 (US$1,500 to US$15,000)

These fines can be combined with orders for suspension of business, revocation of the business licence and/or detention.

Commentary

Multi-national corporations who provide either services or products within China will need to store personal information and important data which has been collected or generated within China and will therefore need to comply with the new Measures and Guidelines. However, at the time of writing these remain in draft form, and a third draft is believed to be in circulation but has not yet been published. Compliance is required by 31 December 2018, when the data transfer regime is due to come into effect. Companies must therefore move swiftly to be ready for this deadline. There are significant challenges ahead and the cost of compliance is likely to be high. In addition, the concept of "important data" continues to be less than precise and will necessarily increase the risk of exposure to criminal and, possibly, civil liability. This is more so the case since the regulatory authorities retain discretion as to how the term "important data" is to be interpreted.

ROSIE NG
Consultant, Hong Kong
T +852 3983 7792
E rosie.ng@hfw.com

Brexit: Technical Notice on No-Deal consequences for data protection

The Department for Digital, Culture, Media & Sport has published a Technical Notice on how the collection and use of personal data would change if the UK leaves the EU in March 2019 with no deal. The Technical Notice is one of a series aiming to provide guidance on how to prepare for a no-deal scenario.

This Technical Notice takes the position that, in the event of a no-deal Brexit, there would be no immediate change in the UK's own data protection standards. This is said to be because the Data Protection Act 2018 would remain in place and

the European Union (Withdrawal) Act 2018 would incorporate the General Data Protection Regulation ((EU) 2016/679) into UK law to sit alongside it. On this basis, it is said that it would remain permissible to send personal data from the UK to the EU. The Technical Notice adds, however, that the UK government will keep the position "under review".

For its part, the European Commission has taken the position that an adequacy decision cannot be made until the UK is a third country.

The UK government has said that it will continue to push for close collaboration between the Information Commissioner's Office and EU data protection authorities.

The Technical Notice may be viewed at: https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal

For further information from HFW on the consequences of the proposed exit of the UK from the EU in March 2019, see: http://www.hfw.com/Brexit

BEN ATKINSON
Senior Associate, London
T +44 (0)20 7264 8238
E ben.atkinson@hfw.com

UK: FCA expectations of brokers on due diligence of insurers

The FCA's recent Regulation Roundup newsletter set out the obligation on insurance brokers to carry out adequate due diligence on insurers, the aim of which is to prevent risk to customers in the event that an insurer fails and is unable to pay claims.

The FCA expects insurance brokers to demonstrate that they have carefully considered the insurers with whom they place their customers' business. The FCA has given guidance as to what brokers should consider as part of their due diligence:

- Insurers' Solvency and Financial Condition Report, to review the solvency coverage percentage;
- FCA and Financial Ombudsman Service (FOS) complaints data, to give an indication as to how an insurer treats its customers;
- Audited accounts;
- BIBA's Litmus Test, an online facility which is free for BIBA members to use, which provides some financial analysis of unrated insurers and a comparison of financial ratios against the wider insurance market;
- FCA Register, to see whether an insurer has passported in on a branch or services basis. UK firms and firms passporting in on a branch basis are automatically covered by FOS; firms passporting on a services basis can elect to come under the voluntary jurisdiction of the FOS. Brokers should check whether an insurer is covered by FOS. If it is not, the broker is expected to check whether there is a dispute resolution scheme in the home state, and whether UK customers are covered by that scheme.

Brokers are expected to give clear details as to the identity of the insurer in the literature they provide to their customers, importantly the insurer itself rather than the Managing General Agent behind it. It is key that customers have the information available to them to make informed decisions as to where their insurance is being placed.

The FCA intends to do further work to verify that insurance brokers are carrying out appropriate due diligence on the insurers with whom they place their customers' business.

CIARA JACKSON
Associate, London
T +44 (0)20 7264 8423
E ciaria.jackson@hfw.com

UK: Migration Advisory Committee report on immigration post-Brexit

The Migration Advisory Committee (MAC) recently published a hotly anticipated report commissioned in July 2017 by then Home Secretary Amber Rudd. The report was commissioned to provide a study and recommendations on the impacts of EEA immigration to support the design of a new immigration system post-Brexit.

The report outlines the impacts of immigration in areas such as the

CIARA JACKSON
ASSOCIATE

"Brokers are expected to give clear details as to the identity of the insurer in the literature they provide to their customers, importantly the insurer itself rather than the Managing General Agent behind it. It is key that customers have the information available to them to make informed decisions as to where their insurance is being placed."

labour market, productivity and the community. The report's findings have been hailed as "myth-busting" by the press, including its conclusion that migration has little or no impact on either employment levels or wages of UK workers.[1] Its principle recommendation is for a "less restrictive regime for higher-skilled workers than lower-skilled workers in a system where there is no preference for EEA over non-EEA workers".[2] The MAC also recommends abolishing the cap on high-skilled workers, describing it as "uncertain" for employers and making "little sense".[3]

The MAC's findings were presented to the Cabinet on 24 September 2018 by MAC chairman Professor Alan Manning. As a result, the Cabinet unanimously voted to support a system based on skills rather than nationality. However, the Cabinet's vote represents only an agreement in principle. In his introduction to the report, Professor Manning stated that the report's findings assume that UK would be "in a position where it is deciding the main features of its immigration policy", with immigration not forming part of the negotiations between the EU and the UK. The reluctance of the Cabinet to provide a firm resolution to implement the findings set out in the Report recognises that the fate of EU migrants working in the UK is likely to depend on the wider Brexit deal.

The Financial Times observed that the report supported views previously expressed by Theresa May and Sajid Javid in relation to the benefits of high-skilled immigration versus low-skilled immigration.[4]

LIZZIE GRAY
Associate, London
T +44 (0)20 7264 8752
E lizzie.gray@hfw.com

Additional research by Rosa Pritchard, Trainee Solicitor

2. MARKET DEVELOPMENTS

UK: Global space industry growth under new UK government proposals

Proposals put forward by the UK government have revealed its aim to secure a 10% share of the global space sector, an increase of 3.5%, by 2030. In doing so, new UK space ports would be built, which in turn would allow for a greater provision of satellite services such as low-gravity spaceflights. This presents new opportunities for space insurers within the London market – as Chris Gibbs, leader of the space team at AmTrust at Lloyds points out, "the UK Space Agency estimates UK spaceports could be worth as much as £3.8 billion to the UK economy over the next decade".

At present, the global space sector is estimated to be worth £40 billion, although only about 40 insurers exist in this class of business. Gibbs notes that "some of the smaller risks get soaked up in the domestic markets around the world, but we see the larger international risks and a variety of domestic risks. The largest we've seen had a value of circa $650 million, but the average risk is more like $250 million. Regular space risks we see in London provide various services ranging from communications satellites to broadband services to data transfer and earth imaging satellites".

The news of the proposals follows the recent statement from the government that £92 million will be invested in a project to develop an alternative to the EU's Galileo satellite system, which will no longer be available to the UK after its exit from the EU.

LUCINDA RUTTER
Associate, London
T +44 (0)20 7264 8226
E lucinda.rutter@hfw.com

3. HFW PUBLICATIONS AND EVENTS

HFW Briefing: Brexit – Impact of a "no-deal" on English disputes with EU counter-parties

Nicola Gare (Professional Support Lawyer, London) considers the UK Government guidance on how disputes will be dealt with in the event of the UK exiting the EU without first having agreed a framework with the EU for ongoing civil judicial cooperation. Read the briefing at http://www.hfw.com/Brexit-impact-of-a-no-deal-on-English-disputes-with-EU-counter-parties.

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741926/Final_EEA_report.PDF (see page 9)

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741926/Final_EEA_report.PDF (see page 5)

3 Ibid

4 https://www.ft.com/content/bd2fbcc6-bb21-11e8-94b2-17176fbf93f5