MACFARLANES JUNHE | 君合律师事务所

DATA PROTECTION CONSIDERATIONS IN COMMERCIAL ARRANGEMENTS BETWEEN THE EU AND CHINA

COMMERCIAL

INTRODUCTION

This article explores the data protection considerations required for business arrangements taking place between entities based in the EU and China involving the transfer of personal data, whether that data is central to the transaction or not. It analyses the subject from the perspective of both jurisdictions to draw a comparison between current approaches and a view as to the future development of this very topical area of law.

EUROPE [1]

It is true that the more straightforward manufacturing trades between these two economies rarely involve data protection and privacy issues. However, in light of China's commitment to the further and future development of its economy as identified in its 12th Five Year Plan to a position higher up the value chain, including in relation to technology and services, transfers of personal data (within the EU Directive definition of the term) will necessarily rise. If the key criteria of pricing, language and contractual certainty are satisfied, then the continued result of globalisation will be that yet more personal data will be processed in countries far from the domicile of the data subject. The greatest uncertainty is whether the security of such personal data will be respected.

The core position under the EU Data Protection Directive (95/46/EC) is that data cannot be transferred out of any EU member state to China without there being a guarantee that the recipient will treat the data under a regime providing equivalent protection to that provided in the EU member state of origin. This applies as much to group companies as for unrelated parties. In the case of China, because it is not acknowledged by the EU as a destination which provides an adequate level of data protection for the purposes of international transfers[2] then for one-off deals, a so-called "Model Contract" provides the solution to allow the transaction to progress. Exemptions from the prohibition on international transfers do exist, and in particular that the transfer is "necessary" for the performance of the contract, but this exemption will be interpreted narrowly: transfers that take place simply to take advantage of advantageous offshore pricing will not viewed as "necessary".

As an EU-domiciled transferor, a data controller (owner) will retain obligations to data subjects which it will need to replicate on a contractual basis with its Chinese counterparty, trusting in the local judicial system to provide an adequate safeguard. If this is not in place, then that transferor will remain at risk of individual claims or collective action from authorities for a failure to protect data. The current proposals from the EU to increase fines to 2 per cent of worldwide turnover mean that such rules need to be considered with great care.

Are data transfers between the EU and China a distant reality or more firmly anchored in the present? On 30 June, 2012 a group of scientists and researchers successfully demonstrated data transfer at a rate of almost 10 Gigabits per second over a new link connecting US and China research and education networks (equivalent to moving more than 5,400 Blu-ray discs in a single day). So the infrastructure is clearly there, and the development of academic links and research opportunities is a strong indicator that the market opportunities for transfers of increasingly commercially valuable data exist.

Examples of data protection matters arising in relation to cross-border transfers from or to China are rare. However, the 2012 case of the investigation by the Hong Kong data protection authorities into the transfer from Macau to the US of personal data by a company in the Asian business unit of Las Vegas Sands indicates that there might be a blueprint for a domestic data protection regime. The sheer size of the jurisdiction means that it will take considerable resource and determination for China to put such a regime in place as well as to support it judicially. However, for those in the services industries for whom sending data to China is (or would be) a key part of their everyday business, the development of a comprehensive regime could prove to be an important step in mitigating risk factors involved in data transfers to the jurisdiction.

CHINA

In summary, the EU model of personal information protection law is not in place yet in China. China has not enacted a single law specifically addressing the collection, storage, transmission and operation of personal information, and has not yet entered into any treaty with EU or any sovereignty similar to the EU-US safe harbor understanding. However, the *Civil Code* (1987) and *Tort Liability Law* (2010) provide legal recourse for infringement of privacy rights. There are also scattered provisions in the People's Republic of China (PRC) laws generally addressing the protection of personal information, typically regulating a specific industrial sector such as the telecommunications sector, or relating to certain information of a specific nature, such as individual financial credit information, employee information, consumer information, and medical records.

Therefore, although at present there are no specific legal requirements for the transfer of personal information within China itself, the cross-border transfer of personal information from China to other jurisdictions is subject to the general privacy

[1] We have not considered regulatory or common law confidentiality in this section, although they form a key element of any decision-making process.

[2] Argentina, Canada, the Channel Islands, Israel and Switzerland and a few others currently have this status.

requirements under civil law. Where the personal information to be transferred is of a specific nature, there are also explicit requirements under industrial regulations and rules.

For example, in the heavily-regulated banking industry, the processing of personal information collected by commercial banks is administered by stringent rules. The People's Bank of China specially requires that personal financial information collected in China must be stored, handled and analysed within the territory of China, and unless otherwise stipulated, banks are not allowed to provide domestic personal financial information overseas. Another example is the transfer of employee information, which is very sensitive in practice and requires delicate handling despite provisions regarding employee information being comparatively simple at present.

In addition to stipulations under civil law and industrial regulations, disclosing information to an offshore entity is strictly prohibited if such information involves State secrets of the PRC. This issue has become highly sensitive recently where Chinese subsidiaries of US companies and companies listed in the US are requested to provide information to the US authorities or US affiliates in relation to FCPA or SEC investigations. Under the *State Secrets Protection Law* (1989) and the *Measures for Implementing the State Secrets Protection Law* (1990), without approval from competent governmental authorities, no documents or materials containing State secrets are allowed to be carried, transmitted, posted or transported outside China. However, the term "State secrets" is broadly defined, covering extensive matters such as major decisions on state affairs, national defense and activities of the armed forces, diplomatic activities and foreign affairs, national economic and social development, science and technology, activities safeguarding national security, and the investigation of criminal offences. The lack of an explicit list or guidelines specifying what information constitutes State secrets or procedures to recognise State secrets has contributed to the extreme difficulty in practice in dealing with information which might be considered as containing State secrets.

It is also worth mentioning that the *Information Security Technology Guide for Personal Information Protection within Information System for Public and Commercial Services* (the Guidelines) was issued on 15 November 2012, and became effective from 1 February 2013. The Guidelines, however, do not serve as a statutory law but a non-mandatory national standard. Nevertheless as many important internet service players have been participating in the process of drafting the Guidelines, such Guidelines are expected to be observed by or at least used as reference in establishing internal rules by many industrial players, and some believe the Guidelines may serve as basis for future legislation on personal information protection. The Guidelines set out both general principles and specific requirements with respect to the collection, processing, transmission, utilisation and management of personal information in various information systems. In particular, in respect of cross-border transfer of data, the Guidelines provide that in the absence of explicit law or regulation, and without the approval of the industrial administrative authority, a Chinese data controller should not transfer any personal information to a data controller registered overseas. Although such requirement is not mandatory, it reflects that attitude of the governmental authorities who have participated in the issuance of the Guidelines and we would expect there may be increasingly strict legal requirements in this regard in the future.

Although the *Personal Information Protection Law* was reported as drafted by academia and submitted to the State Council for discussion in 2008, there is no further news on the specific timeline for discussion or enactment of this piece of law. Even though a unified law may still take some time, governmental authorities in China such as the Ministry of Industry and Information Technology (MIIT) are paying more attention to this issue given several recent cases of personal information leakage. For example, MIIT issued the *Regulation on Personal Information Protection of Telecom and Internet Users* on 16 July, 2013, which will take effect from September, 2013. Under this new regulation, MIIT is expected to gradually strengthen its administration over telecom operators in the field of personal information protection.

CONTACT DETAILS
If you would like further information or specific advice please contact:

RUPERT CASEY - MACFARLANES
DD: +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

MARISSA DONG - JUN HE
DD: +86 10 85191300
dongx@junhe.com

AUGUST 2013

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT
T: +44 (0)20 7831 9222 F: +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com