SEYFARTH SHAW

China Employment Law ALERT

New Data Privacy Obligations for Employers

The National People's Congress Standing Committee has now finalised the new ***Cyber Security Law*** ("**CSL**"), to take effect on 1 June 2017. The fast development of the internet in China has caused a rapid escalation of security issues in China, such as the security of the data of internet users, the management of websites and e-commerce, and all types of cybercrimes. The CSL is intended to address significant gaps in protections around personal data and security in China. The CSL for the first time introduces comprehensive data privacy protection in China and imposes obligations on companies who handle personal information via electronic means.

The CSL applies to all personal information that is processed electronically, but in this alert we focus on the implications for employee data.

Employee data in China: what is the current state of play?

Employers' current obligations with respect to employee data in China are far from clear. Employers are required to "keep employees' personal information confidential and not to publicize personal information without the consent of the employee" (under the ***Regulations on Employment Services and Employment Management***, issued by the Ministry of Labour and Social Security of the PRC in 2007). Similarly, the PRC ***Criminal Law*** and ***Tort Liability Law*** provide that mishandling of personal information and individual privacy can attract criminal and financial sanctions. However, the concept of "personal information" is not defined under Chinese law, making it difficult for employers to be confident that they are compliant.

The CSL: a clearer picture

With the introduction of the CSL, employers will now have clarity as to what constitutes personal information and more clarity as to what steps need to be taken to safeguard data.

The CSL defines personal information broadly, as all types of information recorded by electronic or other means that can identify an individual either in itself or in combination with other information, including but not limited to a citizen's name, date of birth, ID card number, personal biometric information, address and telephone number. The CSL applies to information collected, stored or transmitted electronically.

The CSL places obligations on "cyber service providers", which are defined as the owners and operators of websites and servers, and internet service providers. This would capture employers in their handling of electronic employee data, including personnel files saved onto internal or external servers and information shared by email. Responsibility may in some cases be shared between the employer and a third party service provider who provides the employer's servers or hosts its website. Importantly, the CSL provides express obligations on a cyber service provider to obtain individual consent for the handling of personal information, and to maintain the security of and prevent unauthorised disclosures of personal information.

Where there is a breach, the cyber service provider may be fined, may be required to close a website which breaches the CSL, or may even have its license revoked.

What does this mean for employers?

Unsurprisingly, given this is a new area for the Chinese legislators, the picture is not yet clear, in particular how a breach would be enforced. Would the principle of shutting down an external website that breaches the CSL translate to restricting an employer from handling employee data electronically, in the event of a breach? As is typically the case in China, the new law lays down general principles which will then require interpretation by the Courts, and potentially separate government guidance.

What is apparent however is that there is a new focus on data privacy in China, and employers will need to review their employment documentation and employee notifications, as well as putting in place adequate security procedures to ensure compliance going forward.

In term of next steps, employers should be ready to take the following actions by June 2017 when the CSL comes into force:

- Most importantly, the employer needs to have obtained individual employee consent for the handling of personal information;
- Before collecting and using personal information, the employer needs to issue an employee notice giving details of what personal information will be collected, and how it will be stored and used;
- More fundamentally, employers should review the security of their IT systems to guard against unauthorised disclosures of personal information.

If you would like further information, please contact Wan Li at *lwan@seyfarth.com*, Darren Gardner at *dgardner@seyfarth.com*, or any member of our International Employment Law Practice.