COVINGTON

COVINGTON & BURLING LLP

E-ALERT | International Employment Law Update

October 20, 2014

RUSSIA

Accelerated commencement date for law requiring that personal data of Russian citizens be stored and processed inside Russia

A new law signed on 21 July 2014 will require that all personal data of Russian citizens be stored and processed on servers or databases located within Russia. Organisations that violate the law would be listed on a Register of violators, and the government may order the network provider to block access to the company's network or website.

The new law was scheduled to come into effect in September 2016, but the Russian Parliament is pushing forward legislation to accelerate the commencement date to 1 January 2015, with no transition period.

Important questions remain about the meaning and enforcement of the law. For example, it is not clear whether storage and processing of Russian citizens' data must be done *solely* on Russian databases or whether organisations may transfer personal data cross-border for storage and processing, while maintaining duplicate databases in Russia.

Existing Russian laws already regulate the collection, use, and disclosure of personal data. Additional restrictions apply to employers' use of employee personal data under the Russian Labour Code.

SINGAPORE

New restrictions on collection and use of personal data are now in effect

On 2 July 2014, the final provisions of Singapore's Personal Data Protection Act of 2012 came into effect. Under the law, organisations must (1) obtain consent before collecting, using, or disclosing the personal data (affirmative consent is sometimes required), (2) ensure consent has been obtained for any personal data received through third parties, (3) implement reasonable security arrangements to protect personal data from unauthorised use or disclosure, (4) respond to individuals' requests for access or correction of their personal data, subject to certain exceptions, and (5) designate at least one Data Protection Officer to be responsible for ensuring compliance, although this function may be outsourced.

The law applies to all personal data collected, used, or disclosed in Singapore, including employee data collected for HR purposes. The law prohibits transfer of personal data outside Singapore unless the entity receiving the data provides a comparable standard of protection.

UNITED KINGDOM

Mandatory equal pay audits come into effect

On 1 October 2014, the Equality Act 2010 (Equal Pay Audits) Regulations 2014 came into effect, giving employment tribunals authority to order employers to undergo equal pay audits if they are found to have violated equal pay laws. An employer who commits an equal pay breach will be required to document thoroughly its gender pay information, the reasons for any differences in pay, and its plan for avoiding additional equal pay breaches. Once the tribunal approves the audit, the employer must publish the audit on its website for at least three years.

The Government's Impact Assessment estimates the cost of an audit to be over £13,000, and it could be far higher for large employers. However, the number of audits actually performed is likely to be quite small.

First, only a small percentage of equal pay claims lead to a finding of an equal pay breach because many claims settle prior to a final hearing or are unsuccessful. And the risk of being forced to carry out an audit will likely give employers additional incentive to settle.

Second, businesses with fewer than ten employees ("micro-businesses") and businesses that came into existence less than one year before the equal pay complaint are exempt from the audit requirements.

Finally, tribunals are not required to order audits in a number of circumstances, including where the tribunal finds that (1) the employer has undertaken a similar audit of its pay policies in the previous three years, which may apply to many public sector employers; (2) an audit is not necessary because an employer has a transparent pay system; (3) there is no risk of additional equal pay breaches; or (4) the disadvantages of an audit would outweigh its benefits.

AUSTRALIA

High Court finds no implied term of mutual trust and confidence in Australian employment contracts

Australia's High Court in *Commonwealth Bank of Australia v Barker* confirmed that there is no implied term of mutual trust and confidence in Australian employment contracts. The High Court's decision clarifies the previous uncertainty surrounding the existence and extent of such an implied term. Employers will not be subject to claims for damages by former employees for breach of an implied term of mutual trust and confidence in their employment contract in cases where the employers have not followed all the steps required by an internal policy or procedure. The Australian approach can be contrasted with the English one, where the courts have held for many years that an implied term of mutual trust and confidence exists in employment contracts. However, the Australian High Court left open the possibility that such a term may be introduced by the legislator.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our international employment practice group:

United Kingdom

Christopher Walter	+44.(0)20.7067.2061	cwalter@cov.com
Christopher Bracebridge	+44.(0)20.7067.2063	cbracebridge@cov.com
Helena Milner-Smith	+44.(0)20.7067.2070	hmilner-smith@cov.com

United States

Jeffrey Huvelle	+1.202.662.5526	jhuvelle@cov.com
Lindsay Burke	+1.202.662.5859	lburke@cov.com

People's Republic of China

Ning Lu	+86.10.5910.0502	nlu@cov.com