Developments in data protection

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data - Riyadh

Developments in technology (including increased capacity, functionality, and availability), as well as economic and social globalisation, have resulted in new challenges. Social networking sites, location-based services, on-line shopping, cloud computing, smartphones, and other such developments, mean that we leave digital traces wherever we go. If not managed carefully, this personal information can get into the wrong hands – ranging from telemarketers and spammers to fraudsters and stalkers.

In this article, we outline some notable developments in data protection law in the European Union, the Dubai International Financial Centre and Singapore.

Proposal for new EU Data Protection Regulation

The European Commission has driven the development of policy and law relating to the protection of personal information. The approach taken in Europe has been influential around the world. Under EU law, everyone has the right to the protection of personal information. It can only be gathered legally under strict conditions, for a legitimate purpose. Persons and organisations that collect and manage personal information must protect it from misuse and must respect certain rights of data subjects.

In January this year, the European Commission published its proposal for a new Data Protection Regulation. The EU's current rules date from 1995, and since then there have been significant changes in technology and the way personal data is accessed stored and used. The proposal for the new Data Protection Regulation is intended to strengthen online privacy rights and boost Europe's digital economy, while addressing complexity, uncertainty and cost that has arisen due to inconsistencies between the ways in which the various member states of the EU have implemented the 1995 rules.

Proposed changes to the current regime include:

- There will be a single set of rules on data protection, valid across the EU. Companies will only have to deal with a single data protection authority located in the member state in which they have their main establishment. Individuals will have the right to refer all cases to the data protection authority in their home country – even when their personal data is processed outside their home country.
- EU rules will apply even if personal data is processed abroad. While this gives people in the EU confidence that their data is protected world-wide, it also makes companies outside the EU subject to EU data protection rules if they offer goods or services in the EU.
- A reinforced 'right to be forgotten' will help people better manage data protection risks online. People will be able to delete their data if there are no legitimate reasons for retaining it.
- Wherever consent is required for data to be processed, it will have to be given explicitly, rather than assumed (as is sometimes the case now). In addition, people will have easier access to their own data and be able to transfer personal data from one service provider to another more easily.
- There will be increased responsibility and accountability for those processing personal data. Companies and organisations must notify the relevant national supervisory authority of serious data breaches as soon as possible.

The proponents of the new system claim it will reduce complexity and uncertainty and, in doing so, reduce compliance costs. In contrast, some voices from industry are highlighting the potential for the new system to result in further bureaucracy and costs – without actually increasing efficiency.

The draft Regulation still needs to pass through the EU political process. The general expectation is that it will come into effect in 2014, subject to any changes that may arise in the course of the political process.

Proposed changes to DIFC Data Protection Law

By way of background, certain provisions of the UAE Penal Code provide the main legal basis for data protection under UAE law. The relevant provisions are essentially pointed at the privacy of the individual, and – being, as they were, drafted in the 1980s – they do not specifically envisage the types of technological advancements that have made data protection so topical. Other federal laws, including the Medical Liability Law (Federal Law No. 10 of 2008) and the Credit Information Law (Federal Law No. 6 of 2010) amongst others, restrict the use of personal information in specific circumstances.

In contrast, the Dubai International Financial Centre, a financial services free zone located in the Emirate of Dubai, has its own 'European style' data protection law, applicable in the jurisdiction of the DIFC. The Data Protection Law 2007 (DIFC Law No. 1 of 2007) prescribes rules and regulations regarding the collection, handling, disclosure and use of personal data in the DIFC, the rights of individuals to whom the personal data relates, and the role of the DIFC Authority with regard to data protection. The Data Protection Law embodies international best practice standards, and is broadly consistent with the 1995 EU Data Protection Directive. It is designed to balance the legitimate needs of businesses and organizations to process personal information with the importance of upholding an individual's right to privacy.

Generally speaking, as part of the set-up process in the DIFC, an entity is required to notify the DIFC's Commissioner of Data Protection if it intends to process personal information, including transferring personal information outside of the DIFC. This notification has to be updated when the entity's commercial licence is renewed, or if at any time the entity changes the way in which it will process personal information.

An entity that wishes to process 'Sensitive Personal Data' (being personal information revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life), or that wishes to transfer personal information outside the DIFC to a jurisdiction that is not recognised by the DIFC as offering an adequate level of protection to personal information, needs to seek a permit from the Commissioner of Data Protection.

A number of changes to the Data Protection Law have been proposed recently. Besides miscellaneous amendments aimed at improving drafting and clarity, the key changes to the Data Protection Law can be summarised as follows:

Duty to notify changes: A Data Controller must notify the Commissioner of Data Protection of any changes to the particulars of the Data Controller's notification to the Commissioner. Failure to notify the Commissioner of such changes as soon as possible – and in any event within 14 days from the date upon which the particulars becomes inaccurate or incomplete – is a contravention of the law.

Delegation powers of the Commissioner of Data Protection: The Commissioner may delegate functions and powers to officers and employees of the Dubai International Financial Centre Authority.

General contravention and administrative imposition of fines: The proposed changes set out provisions relating to contraventions of the law and the administrative imposition of fines.

Developments in Singapore

Meanwhile, Singapore is planning to pass a new law that will be known as the Personal Data Protection Act, which is likely to come into effect in the third quarter of 2012.

The current situation in Singapore has some parallels with legal protection of personal information in the UAE. Specifically, there has been no specific data protection law of general application, and the protection of personal information has largely been handled in the context of other more general legal provisions that

protect privacy.

According to the bill, the new law will establish a data protection commission responsible for the administration and enforcement of the law. The law will apply to all private sector organizations in Singapore, and – significantly – will also apply to organizations located abroad that are engaged in data collection, processing and disclosure of such data within Singapore. (This aspect is similar, to some degree, to changes being proposed in Europe.) Organizations will be required to appoint an officer responsible for compliance with the law, and to implement policies and practices to comply with the law. Individuals will be able to request access to their personal data in order to find out how it is being used or collected, and to correct any inaccuracies and seek readdress of suspected breaches of the law. Notably, under the law, Singapore is planning to introduce a "do not call registry" which allows users to register their contact details so that they do not receive unsolicited marketing communications. This process will require would be telemarketers to verify with the registry before sending any messages that the intended recipients number does not appear on the register.

As a small nation committed to developing its knowledge economy, Singapore is an example that UAE might like to follow.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on data protection issues in the Middle East, including in on-shore Dubai and free zones such as DIFC. For any data protection related queries, please contact David Yates (d.yates@tamimi.com) or Nick O'Connell (n.oconnell@tamimi.com)