Data breach notification requirements in the DIFC

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data
n.oconnell@tamimi.com - Riyadh

August 2015

In this article we consider the obligations on data controllers, under the DIFC Data Protection Law, to make formal notification in the event of a breach of personal data.

The Dubai International Financial Centre is a financial services free zone with a European-style data protection regime.

The DIFC Data Protection Law (DIFC Law No. 1 of 2007, as amended) requires data controllers to implement appropriate technical and organizational measures to protect against accidental, negligent or unlawful loss, disclosure or access to personal data, particularly in the context of the processing of sensitive personal data or the transfer of personal data to recipients outside the jurisdiction of the DIFC. Such measures are required to ensure a level of security appropriate to the risks presented by the manner of processing and the nature of the personal data in question. When engaging a data processor to process personal data on its behalf, a data controller is required to select a data processor able to provide sufficient guarantees in respect of the technical and organizational security measures it will apply to such processing.

Significantly, Article 16(4) of the DIFC Data Protection Law states:

In the event of an unauthorised intrusion, either physical, electronic or otherwise, to any personal data database, the data controller or the data processor carrying out the data controller's function at the time of the intrusion, shall inform the commissioner of data protection of the incident as soon as reasonably practicable.

The DIFC Commissioner of Data Protection's expectation regarding the timeframe for reporting a breach is 'as soon as reasonably practicable'. The Commissioner is open to receiving an initial notification giving high-level details of the breach, with a more detailed report and set of remedial actions delivered as swiftly as possible without unjustifiable delays. Based on other timeframes referred to in the DIFC Data Protection Law (albeit in other contexts) there is some likelihood that a period longer than 14 days from the event giving rise to the notification would be considered 'too long', particularly where there was no obvious justification. Acting swiftly is likely to be seen favourable when the Commissioner is considering if any disciplinary action is appropriate.

There is no explicit obligation in the DIFC Data Protection Law with regard to notifying affected data subjects. Despite this, guidance issued by the Commissioner in respect of Article 16(4) indicates that the Commissioner expects that it may be appropriate to notify affected data subjects – and such notification would be taken into account when the Commissioner is assessing the nature of any disciplinary action that it may wish to take in response to the breach.

The Commissioner's guidance mentions that a breach notification should:

- Set out a description of how and when the breach occurred, what personal data was involved and what has already been done to mitigate the risks;

- Give clear and specific advice on what data subjects can do to protect themselves and what it is willing to do to help them;
- Provide a helpline or webpage where data subjects can find out more about what has occurred; and
- Ensure that the notification medium is appropriate and secure (ie. not disclose any further personal data of the affected data subjects).

It also states that, at a minimum, the Commissioner would expect the following to be addressed in a report relating to a breach:

- The type of personal data and number of records compromised;
- The circumstances of the breach;
- The immediate action taken to minimise/mitigate the effects of the breach;
- The details of how the breach is being investigated;
- Whether affected data subjects and the public know, or have been informed, of the breach;
- Whether any other regulatory body has been informed, and its response; and
- Whether any long-term remedial action is being undertaken to prevent future occurrences.

The references to giving 'clear and specific advice on what data subjects can do', and providing 'a helpline or webpage where data subjects can find out more', generally support the view that affected data subjects should be notified of a breach. In contrast, the Commissioner's guidance also alludes to 'whether affected individuals […] have been informed'. This could be read as indicating that it is not always essential to notify affected data subjects of a data breach, and that the Commissioner would be open to taking a case-by-case approach when considering whether such notification is appropriate.

The DIFC's guidance on notifications to the Commissioner in the event of a data breach refers to what the 'data controller' should do. Our view is that this should be read as extending to the 'data processor' (if it is the data processor that is notifying the Commissioner pursuant to Article 16) – although in practical terms our recommendation would generally be for any breach notification to be communicated to the Commissioner via the DIFC-based data controller.

There are a range of other issues that may also need to be considered by a data controller in the DIFC in the event of a data breach. These include whether or not any related transfers of personal data outside the jurisdiction were compliant with the requirements for processing/transferring as set out in the DIFC Data Protection Law, whether or not the Regulator of financial services firms set up in the DIFC will also need to be notified, and whether the data breach should also be notified to the police.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on privacy and data protection matters in the Middle East. For further information, please contact Nick O'Connell – n.oconnell@tamimi.com