Supervisory Visits by the DIFC Commissioner of Data Protection

by Nick O'Connell - n.oconnell@tamimi.com - Riyadh

October 2016

Recent activity by the Dubai International Financial Centre ("DIFC") Commissioner of Data Protection (the "DIFC Commissioner") has attracted attention and caused DIFC licensed entities to review their own personal data processing operations and revisit their DIFC data protection compliance obligations.

Amongst various responsibilities, the DIFC Commissioner is charged with promoting, amongst data controllers in the DIFC, good practices and observance of the requirements of the DIFC Data Protection Law, and promoting greater awareness and public understanding of data protection. These activities can broadly be understood as the supervisory role of the DIFC Commissioner.

In performing its supervisory role, the DIFC Commissioner balances the need to educate the DIFC community about data protection compliance with the practical reality of limited personnel and resources. Over the last few years, the DIFC Commissioner has performed this aspect of its role by way of various relatively low-profile exercises, including 'supervisory visits' and 'notices to produce'.

The 'supervisory visit' scenario typically involves the DIFC Commissioner approaching entities licensed in the DIFC in order to arrange for a meeting at an appointed date. These meetings provide an opportunity for the review of documentation and processes relating to the processing of personal data, and appear more likely to be about ensuring a culture of awareness and compliance than being deeply forensic or judicial in nature.

The types of topics that the DIFC Commissioner might expect to address during a supervisory visit include:

- a general description of the entity, the number of staff, locations in which it operates, and its area of business;
- details of the class of personal data the entity processes, the types of data subjects to which such data relates, and the purposes for which it is processed;
- details of the entity's data protection policies and procedures (including aspects such as the level of security applied, whether disclosure is consistent with the purpose for which personal data was collected, and whether there are procedures for keeping personal data up-to-date);
- an explanation of any data protection training given to personnel, along with information on training materials and records of training conducted;
- details of any periodic reviews and audits of personal data held, to assist in complying with obligations under the DIFC Data Protection Law;
- details relating to the transfer of personal data to other jurisdictions outside the DIFC, and the grounds upon which such transfers are based; and
- any other background material that might be appropriate to demonstrate the entity's compliance with the DIFC Data Protection Law.

In contrast to the supervisory visit approach, the 'notice to produce' scenario involves the DIFC

Commissioner approaching entities licensed in the DIFC and directing them to provide greater detail on the substance of their data processing activities. In the past, this has involved what could broadly be described as a 'bulk mail out', whereby a significant number of entities (anecdotal reports indicate more than 100 in February 2016) received such letters, specifying a deadline by which they were required to provide a substantive response.

In both the supervisory visit scenario, and the notice to produce scenario, entities approached by the DIFC Commissioner often wonder why they have been singled out for attention. While we cannot be certain how the DIFC Commissioner identifies appropriate targets, the most obvious explanation appears to be irregularities with the content of the notifications previously filed by such entities with the DIFC Commissioner. (The filing of a notification of personal data processing activities is a requirement of all entities licensed in the DIFC, and this needs to occur at the time of initial licensing and at the time of each subsequent renewal, as well as at any time in the interim when the manner of processing changes from that already notified.)

Anecdotally, it would seem that the entities that received 'notices to produce' were entities that had previously advised the DIFC Commissioner, via their annual data processing notifications, that they were not processing any personal data in the course of their activities. (The likelihood of an entity not processing any personal data is very limited, so a 'negative' notification would likely benefit from closer scrutiny.) In the case of entities who were the targets of 'supervisory visits' by the DIFC Commissioner, such entities also appear to have had discrepancies in the content of their notifications that resulted in greater scrutiny being applied.

There is a legal obligation on entities licensed in the DIFC to comply with the DIFC Data Protection Law. The 'risk' of coming to the attention of the DIFC Commissioner should not be the driver for compliance with the law, but in practical terms the DIFC Commissioner's supervisory activities may well be a catalyst for many DIFC entities to review their data protection compliance obligations and make sure that everything is in order. The reality is that DIFC data protection notifications are, in many instances, not given appropriate attention and treated simply as a 'box ticking' exercise. We are aware of instances where poorly considered notifications have simply been renewed annually without any further thought.

To ensure compliance, we recommend that all entities operating in the DIFC undertake a full audit of their own personal data processing operations so as to ensure that they are compliant with DIFC Data Protection Law requirements, including with regard to the substance of their activities and with regard to the official notification that needs to be filed with the DIFC Commissioner.

The DIFC Data Protection Law provides for significant penalties for non-compliance. While the DIFC Commissioner appears, to date, to have been generous in focussing on developing a culture of awareness, there can be no guarantees that failure to comply will not result in penalties in appropriate circumstances.

The Abu Dhabi Global Market ("ADGM") has only recently been established, and the ADGM Data Protection Regulations only came into effect in October 2015. In this context, the ADGM Registrar is still at a very early stage in establishing processes, but in due course we would expect that it will also become active in ensuring that ADGM licensees comply with the data protection obligations imposed on them pursuant to the ADGM Data Protection Regulations.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on data and data protection issues throughout the Middle East, including in the Dubai International Financial Centre, the Abu Dhabi Global Market and Dubai Healthcare City. For further information please contact Nick O'Connell (n.oconnell@tamimi.com) or Sana Saleem (s.saleem@tamimi.com).