Requirements for data protection officers in Dubai International Financial Centre

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

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

As of July 2020, the Dubai International Financial Centre, a financial services free zone in the Emirate of Dubai, has a new data protection law, the Data Protection Law 2020 (the 'DIFC Data Protection Law'). One key topic relevant to data controllers and data processors subject to the DIFC Data Protection Law is the question of whether or not it is compulsory to appoint a Data Protection Officer ('DPO'). A DPO is someone appointed by a data controller or data processor to independently oversee certain data protection operations. In this article, we consider this point, and provide further information on related issues, including who can fulfil the DPO role, and the obligations incumbent on a DPO.

Is there a statutory requirement to appoint a DPO?

There is a requirement to appoint a DPO in certain circumstances. Certain DIFC Bodies (such as the DIFC Authority, the Dubai Financial Services Authority, and the DIFC Courts (with a limited exception), are required to appoint a DPO. Data controllers and data processors that are performing certain 'high risk' personal data processing activities must also appoint a DPO. There may be circumstances where the Commissioner of Data Protection requires a data controller or data processor, not falling into either of these categories, to appoint a DPO. (If a data controller or data processor is subject to the statutory requirement to appoint a DPO, it must submit an annual assessment of its data processing activities to the Commissioner of Data Protection, in the form prescribed by the Commissioner.)

The type of 'high risk' personal data processing activities that trigger the requirement to appoint a DPO include:

- processing that utilises innovative technologies or methods, with a material increase in risk to security or to data subject rights;
- a considerable amount of personal data will be processed and such processing is likely to result in a high risk to the data subject (e.g. due to the sensitivity of the data, or risks relating to security, integrity or privacy of the data);
- the processing will involve a systematic and extensive evaluation, based on automated processing, on which decisions are based that produce legal effects or similarly significantly affect the natural person; or
- a material amount of 'special categories' of personal data (e.g. personal data revealing or concerning racial or ethnic origin, communal origin, political views, religious beliefs, criminal record, trade-union membership and health or sex life) is to be processed.

Data controllers and data processors subject to the DIFC Data Protection Law should consider whether they fall within any of the types of entities that must, by their nature, appoint DPOs. Otherwise, they should assess their personal data processing activities to determine whether they fall into the 'high risk' category that necessitates the appointment of a DPO. Based on guidance issued by the Commissioner of Data Protection, it can be concluded that the threshold for 'high risk' personal data processing is not high; there is some likelihood that many data controllers and processors operating in DIFC may need to appoint a DPO.

Even if a statutory requirement to appoint a DPO does *not* apply, a data controller or data processor subject to the DIFC Data Protection Law still needs to clearly allocate responsibility for data protection compliance within its organisation. It is also permissible for a data controller or data processor to appoint a DPO in circumstances where it is not strictly required to do so.

Who can be a DPO?

A DPO could be someone employed within a data controller or data processor, or within the corporate group of the data controller or processor (where the data protection officer role is managed centrally across a corporate group), or a third party service provider.

An individual acting as DPO to a corporate group can be based outside the UAE; otherwise, DPOs need to be resident in the UAE. (To the extent that a DPO could be a corporate third party service provider, it is our understanding that such service provider would need to be an entity licensed to operate in the UAE.)

A DPO needs to be familiar with the requirements of the DIFC Data Protection Law, and ensure that the data controller or data processor complies with such requirements. A DPO needs to be able to act independently and under his or her own authority, and have sufficient resources to discharge the duties of a DPO effectively, objectively and independently. A DPO needs to have timely and unrestricted access to information within the data controller or data processor to perform the duties of the DPO, and to have direct access to senior management. A DPO can perform other roles within a data controller or data processor, and for many organisations it would not be uncommon for the DPO role to be filled by a legal or compliance specialist, or an HR specialist, depending on the size and nature of the organisation.

Importantly, a DPO needs to be able to fulfil a variety of specific tasks set out in the DIFC Data Protection Law. These include:

- monitoring its data controller's, or data processor's, compliance with the DIFC Data Protection Law, and any policies relating to the protection of personal data (such as training of staff involved in personal data processing operations, and the data protection audits);
- advising relevant personnel of the data controller or data processor of applicable obligations pursuant to the DIFC Data Protection Law and other data protection considerations (such as foreign requirements with extra-territorial effect), and on data protection impact assessments;
- co-operating with the Commissioner of Data Protection, and acting as the Commissioner's contact point for issues relating to personal data processing;
- addressing the Commissioner's findings, recommendations and directives, etc.; and
- acting as the contact point for data subjects who wish to exercise their rights under the DIFC Data Protection Law.

What next?

Data controllers and data processors that are subject to the DIFC Data Protection Law need to determine whether or not they are subject to the statutory requirement to appoint a DPO. If a DPO is required, the DPO needs to have the competencies and status necessary to discharge his or her duties, as contemplated in the DIFC Data Protection Law. One of the first responsibilities of the DPO will be to ensure that the annual assessment is submitted as a matter of priority.

For further information, please contact Nick O'Connell (n.oconnell@tamimi.com) or Andrew Fawcett (a.fawcett@tamimi.com).