DIFC DP Law: Appointing a Data Protection Officer

Charlotte Sutcliffe - Associate - Digital & Data
- Dubai International Financial Centre

The Dubai International Financial Centre ("**DIFC**"), has issued a new Data Protection Law DIFC Law No. 5 of 2020 ("**DIFC DP Law**"). This law applies in the jurisdiction of the DIFC only

In this article, we focus on the circumstances under which controllers (i.e. entities that control the processing of personal data) and processors (i.e. entities under the direction of a third party to process personal data) must appoint a Data Protection Officer (DPO).

What is a DPO?

A DPO is defined under the DIFC DP Law as an officer appointed by a controller, joint controller or processor to independently oversee relevant data protection operations in the manner set out under the DIFC DP Law. In practice, a DPO is an individual appointed by the entity whose job it is to oversee an entity's compliance with the DIFC DP Law.

When should a DPO be appointed?

It is mandatory for a DPO to be appointed by:

1. DIFC Bodies, other than the Courts acting in their judicial capacity; and
2. a controller or processor performing 'High Risk Processing Activities' on a systematic or regular basis.

Under Article 16(3), the DIFC Commissioner of Data Protection ("Commissioner") may also require a controller or processor to designate a DPO.

Otherwise a controller, joint controller or processor may voluntarily designate a DPO under Article 16(1).

A 'DIFC Body' includes the Commissioner, DIFCA, DFSA, DIFC Courts, and any other person, body, office, registry or tribunal established under DIFC Laws or established upon approval of the President of the DIFC that is not revoked by the DIFC DP Law or any other DIFC Law.

High Risk Processing Activities

A 'High Risk Processing Activity' is the processing of personal data where one or more of the following applies:

- processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a data subject or renders it more difficult for a data subject to exercise his or her rights;

- a considerable amount of personal data will be processed (including staff and contractor personal data) and where such processing is likely to result in a high risk to the data subject, including due to the sensitivity of the personal data or risks relating to the security, integrity or privacy of the personal data;
- the processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling (i.e. automated processing of personal data to evaluate the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the person's performance at work, economic situation, health), and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
- a material amount of special categories of personal data is to be processed (i.e. personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record).

The Commissioner has published policy guidance to assist controllers and processors to determine whether any of their business activities fall within this definition.

Must a DPO be an employee of the Controller in the UAE?

A DPO must reside in the UAE unless he or she is an individual employed within the organisation's group and performs a similar function for the group on an international basis. The role of a DPO may be performed by a member of a controller's or processor's staff, an

individual employed within a controller's or processor's group in accordance, or by a third party under a service contract. A group may appoint a single DPO provided that he or she is easily accessible from each entity in the group. A DPO may hold other roles or titles within a controller, processor or in a group, and may fulfil additional tasks and duties other than those described in the DIFC DP Law.

What should a DPO do?

A DPO is the data subject's and the Commissioner's first point of call about any data protection related issues. It must have knowledge of the DIFC DP Law and its requirements and shall ensure a controller or processor monitors compliance with the DIFC DP Law.

General duties

A DPO must:

- be able to perform his or her duties and tasks in an independent manner, and be able to act on his or her own authority;
- have direct access and report to senior management of the controller or processor;
- have sufficient resources to perform his or her duties in an effective, objective and independent manner;
- have timely and unrestricted access to information within the controller or processor organisation to carry out his or her duties and responsibilities under the DIFC DP Law;
- monitor a controller or processor's compliance with the DIFC DP Law and any other data protection or privacy-related laws or regulations to which the organisation is subject within the DIFC;

- be properly involved in a timely manner, on all issues relating to the protection of personal data and be given sufficient resources necessary to carry out the role;
- be free to act independently;
- ensure any other tasks it undertakes do not result in a conflict of interest or otherwise prevent the proper performance its role as a DPO; and
- conduct necessary training for staff members in the controller or processor to ensure they are aware of their obligations under the DIFC DP Law.

Conducting assessments

Where a controller is required (and has not elected) to appoint a DPO, the DPO shall undertake an assessment of the controller's processing activities, at least once per year, which shall be submitted to the Commissioner, which should include information such as whether it intends to undertake high risk processing activities (such an assessment is referred to as a DPO Controller assessment)

A data protection impact assessment is an assessment of the impact of the proposed processing operations on the protection of personal data, considering the risks to the rights of the data subjects concerned.

A DPO, where appointed, shall be responsible for overseeing data protection impact assessments.

Prior to undertaking High Risk Processing Activities, a data protection impact assessment has to be carried out regarding on the impact of the proposed processing operations on the protection of personal data, considering the risks to the rights of the data subjects concerned.

Information provision

A controller who has appointed a DPO must provide any data subject from whom it obtains personal data with the contact details of the DPO.

Consequences for failing to appoint a DPO

Failing to appoint a DPO where required under the DIFC DP Law could result in a fine of up to US$50,000.

Comparison with the GDPR

The obligation to appoint a DPO is substantially similar under the EU General Data Protection Regulation ("**GDPR**"). However, there are a few additional aspects to designating a DPO under the DIFC DP Law, including:

- If a controller / processor is not required to appoint a DPO, it must still allocate responsibility for the oversight and compliance regarding the entity's data protection duties
- A controller or processor could be required to appoint a DPO by the Commissioner
- A DPO is required to assess the controller's processing activities annually and provide the findings to the Commissioner

- The DPO needs to be in the UAE unless the DPO is an individual employed within the Controller's group of companies and performs a similar function for the group on an international basis.

Conclusion

The DIFC DP Law provides for entities processing personal data to appoint a DPO for overseeing that entity's compliance with the DIFC DP Law. In some circumstances, a DPO is mandatory.

It is an important role which is given to an individual so that an entity is more effectively able to manage its obligations under the DIFC DP Law. Compliance with the DIFC DP Law and continuous monitoring is a key task of the DPO.

A DPO has to have sufficient expertise, independence and resources to effectively perform their statutory duties. The DPO should work with the Commissioner in a transparent and cooperative way.

Even if a controller or processor is not required to appoint a DPO under the DIFC DP Law, it must still clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations under the DIFC DP Law, or any other applicable data protection law, within its organisation and be able to provide details of the persons with such responsibility to the Commissioner upon request.

For more information on how we can help, please contact Charlotte Sutcliffe (c.sutcliffe@tamimi.com).