THE NEW DIFC DATA PROTECTION LAW

INTRODUCTION

The Dubai International Financial Centre ("**DIFC**") has issued a new Data Protection Law (the "**DP Law**"), which will come into force on 1 July 2020. The DIFC has announced there will be a grace period until 1 October 2020 to comply with the DP Law. The DP Law will align the DIFC's regulatory framework more closely with international data protection developments, including the EU's General Data Protection Regulation ("**GDPR**") as highlighted in our earlier briefing on the draft law which can be found here.

In this briefing we highlight some of the key features of the DP Law that will affect the data processing operations of companies operating in the DIFC.

Key Changes

- Requirements for processing data outside the DIFC
- Data Protection Officer and Data Protection Impact Assessment
- Stricter consent requirements
- Impact on transfers
- More rights for data subjects
- Notifying data breach to data subjects

Territorial Application

The DP Law applies to:

(a) the processing of personal data by DIFC incorporated entities (regardless of whether the processing takes place inside the DIFC or outside); and

(b) the processing of personal data within the DIFC even if the entity on behalf of whom such data is processed is incorporated outside the DIFC. Processing of data occurs within the DIFC if the means or personnel for processing are situated within the DIFC and if such processing is conducted on a regular basis.

The DP Law may not apply to branches of DIFC incorporated entities outside the DIFC to the extent that those branches do not process personal data within the DIFC.

A DIFC company that outsources its data processing activities to a company (whether within or outside the DIFC) is now required to enter into a formal contract (with certain mandatory provisions) with the data processing company. We anticipate that companies will need to formalise such contracts within the grace period unless a further extension is provided by the regulator.

High Risk Processing Activities

The DP Law introduces the concept of "High Risk Processing Activities" which are summarised below with our suggested examples:

- the use of new technology that increases risk to Data Subjects (e.g. the use of artificial intelligence or machine learning);
- the processing of a "material" amount of special categories/sensitive personal data such as race, health, religion, etc. (e.g. healthcare or insurance providers);

- processing "considerable" amounts of Personal Data that poses a high risk to the Data Subject, for example, on account of sensitivity of Personal Data or risks relating to the security, integrity or privacy of Personal Data; or
- automated processing, including profiling, which leads to decisions with legal effects on natural persons (e.g. online recruitment tools without human intervention).

This definition (in particular limbs 2 and 3 above) could arguably apply to larger companies in the DIFC which process a large amount of their employee's personal data within the DIFC. The DP Law envisaged the DIFC Data Protection Commissioner ("**Data Commissioner**") publishing a non-exhaustive list of activities categorised as High Risk Processing Activities. Such guidance is now available on the DIFC website, and contains specific reference to employers with large payrolls. The guidance is however noted to be non-exhaustive and non-binding.

A processor or controller that engages in High Risk Processing Activities must adopt a more cautious approach to processing. The DP Law requires such companies to carry out regular data protection impact assessments ("**DPIAs**") and to appoint a data protection officer ("**DPO**") before proceeding.

DPO obligations

Controllers or Processors engaging in "High Risk Processing Activities" on a regular basis are required to appoint DPOs. Companies may also elect to appoint a DPO even if they do not engage in "High Risk Processing Activities". Moreover, the Data Commissioner has the power to require companies to appoint a DPO even if they are not conducting High Risk Data Processing Activities. Companies that are in doubt as to whether they conduct High Risk Processing Activities should consider appointing a DPO.

The DPO must ordinarily be resident in the UAE. However, international groups can appoint a single DPO based outside the UAE provided they can fulfil their functions under the DP Law. We anticipate that most international groups may rely on their DPOs in the wider network (e.g. the EU).

DPOs will be required to monitor their company's compliance with the DP Law, any other data protection or privacy-related laws that apply within the DIFC and any policies relating to the protection of personal data and also provide training to staff.

DPIA requirements

Controllers engaging in "High Risk Processing Activities" are also required to carry out DPIAs and the DP Law sets out minimum requirements for a DPIA which are similar to the GDPR. The Data Commissioner may also list processing activities where a DPIA may not be required.

Where a DIFC controller is part of an international group, and another entity in that group has conducted a DPIA which meets the minimum requirements of the DP Law, the DIFC controller may rely on that DPIA. We anticipate that groups who conduct DPIAs under the GDPR might be able to rely on these provided they are current and accurate.

Stricter consent requirements

Consent of the data subject remains a ground on which companies can process personal data. However, the new DP Law adopts a more stringent approach and requires companies to obtain consent in relation to each specific data processing purpose (which is in line with the GDPR). Importantly,

Key New Concepts

- ***Binding Corporate Rules*** - written procedures which regulate the transfer of personal data between members of the same group. Binding Corporate Rules are an avenue for intra-group transfers of personal data out of the DIFC.
- ***High Risk Processing Activities –*** activities that have a greater chance of making personal data vulnerable to unintended disclosure and therefore require additional protections including, conducting a data protection impact assessment and appointing a data protection officer.
- ***DPO -*** data protection officer to monitor compliance with the Proposed Law. International Groups can rely on DPOs in their network.
- ***DPIA –*** data protection impact assessment – international groups can rely on DPIA's conducted in their network if such DPIA's cover the requirements stipulated in the DP Law.

companies have to ensure that such consent remains valid over time. The Data Commissioner's guidance makes it clear that a generic consent clause in standard terms and conditions without specifying the use of such data will not be valid. Equally, if consent is obtained by ticking a box, the associated wording should specify the use of such data.

Impact on data transfers

The DP Law does away with a permit from the Data Commissioner being a valid ground for a data transfer outside the DIFC.

The DP Law retains the concept of permitting data transfers to pre-approved jurisdictions listed on the DIFC website. However, in the context of transfers to other jurisdictions, the DP Law provides companies a larger array of options than the previous law and also detailed guidance as to what constitutes "adequate safeguards" to aid the self-assessment by companies.

The DP Law also allows controllers to have Binding Corporate Rules approved by the Data Commissioner which permit intra-group transfers. Alternatively, intra-group transfers could occur under the legitimate interest ground.

Rights of data subjects

The rights of data subjects remain a core component of the DP Law, with many of the new concepts clearly intended to reinforce the protections surrounding such rights.

Under the DP Law, the list of data subject rights has been expanded. In particular, data subjects shall now have an express right to withdraw consent at any time, as well as the right not only to object to processing, but also to restrict processing in certain circumstances.

Following the implementation of the GDPR in the EU, there was a notable increase in data subject access requests. It remains to be seen if the DP Law will lead to an increase in such requests in the DIFC. If it does, companies will need to create systems to deal with them.

Notification of data breaches

Where a personal data breach is likely to result in a high risk to the security or rights of a data subject, the Controller is required to communicate the personal data breach to affected data subjects as soon as practicable in the circumstances. This is in addition to notification to the Data Commissioner.

Fines

Penalties range between US$20,000 to US$100,000 for administrative breaches. For example, a failure to appoint a DPO if required by the DP Law can attract a maximum fine of US$50,000. In addition, the Data Commissioner has the right to impose a general fine for more serious violations of the DP Law. Controllers and processors may also be liable to pay compensation to data subjects whose rights have been violated.

Conclusion

The DP Law heralds significant operational changes for DIFC Companies who will have to review existing data processing arrangements, update data policies and consent forms and potentially appoint a DPO and conduct a DPIA on a regular basis. We are advising companies on compliance with the DP Law and can help your business navigate these changes.

Additional Rights for Data Subjects

- Right to withdraw consent at any time
- Right to restrict processing in certain circumstances
- No discrimination against a data subject who exercised rights
- No decision affecting data subject based solely on automated process
- More information to be provided by data controllers/processors
- "**Profiling**" – automated evaluation of personal aspects of a natural person (such as to assess work performance, economic situation, health, behaviour, movements and personal preferences). Specific restrictions under the Proposed Law on automatic profiling.

CONTACTS

James Abbott
Partner

T +971 4503 2608
E james.abbott
@cliffordchance.com

Arun Visweswaran
Senior Associate

T +971 4503 2748
E arun.visweswaran
@cliffordchance.com

James Dadford
Associate

T +971 4503 2625
E james.dadford
@cliffordchance.com

Shamim Khan
Trainee

T +971 4503 5529
E shamim.khan
@cliffordchance.com