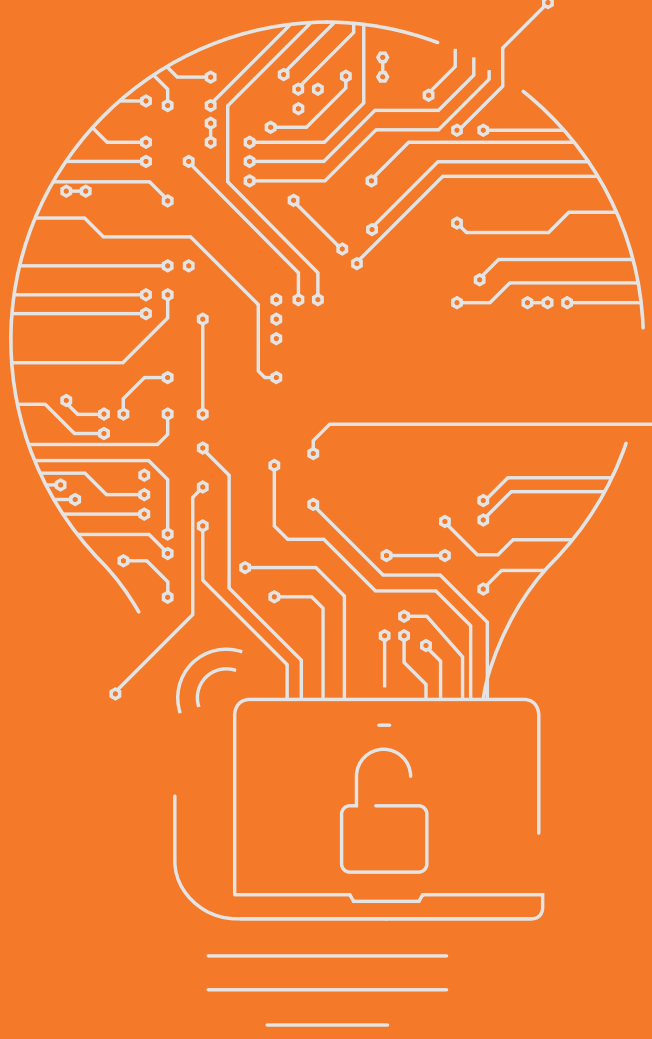


New DIFC Data Protection Law 2020

What you need to know



كلايد اند كو
CLYDE & CO



Introduction



Background and Aims

The new Dubai International Financial Centre (DIFC) Law No. 5 of 2020 Data Protection Law (DPL 2020) replaces the existing data protection law and brings the DIFC more closely into-line with data protection law in Europe, where the General Data Protection Regulation (GDPR) is applicable throughout.

DPL 2020 aims to further DIFC's desire to be recognised internationally as a top-tier jurisdiction for data protection. The law will hopefully prove to be the next step on the road to achieving "adequacy" status as a destination for free transfers of personal data from Europe.



Who is affected?

- Any business registered in the DIFC
- Any business which processes personal data within the DIFC as part of stable arrangements
- Any business which processes data on behalf of either of the above



Timing

The DPL 2020 will come into force on 1 July 2020. The DIFC Commissioner of Data Protection is expected to announce that the law will not be actively enforced until 1 October 2020, giving businesses a four month implementation window to prepare.

Similarities with GDPR

➤ Data protection principles

DPL 2020 reflects the core data protection principles found in the GDPR (fairness, lawful and transparent processing, purpose limitation, data minimization, accuracy, storage limitation, security, accountability) and operates using similar core concepts such as "controller", "processor", "data subject" etc.

➤ Lawful basis for processing

Under DPL 2020, entities can process data based on:

- the consent of the data subject
- performing or entering into contract with the data subject
- compliance with legal obligations on the Controller
- to protect the vital interests of the data subject
- processing for a task in the interests of the DIFC or for the exercise of the DIFCA, DFSA, Court and Registrar's functions or powers
- legitimate interests of the controller or a third party

➤ Special categories of personal data

Under DPL 2020, a further basis is needed to process special categories of personal data. The available grounds are similar to those in GDPR.

➤ Provision of information and record keeping

Data subjects must be provided with information about how data will be processed and used and controllers must keep records of processing activities.

➤ Appointment of a data protection officer

Some controllers and processors will need to appoint a data protection officer, depending on whether they conduct High Risk Processing Activities.

➤ Data processors

DPL 2020 imposes direct compliance obligations on processors and also stipulates mandatory contractual requirements that apply to arrangements between controllers and processors.

➤ Data subject rights

DPL 2020 grants data subjects very similar rights to GDPR, such as the right of access and the right to request deletion. Data subjects are free to withdraw consent to processing.

➤ Transfers out of DIFC

Transfers, including to the UAE onshore, can only take place if:

- the transfer is to a country or international organization that provides an adequate level of data protection as determined by the Commissioner of Data Protection, or
- if appropriate safeguards are put in place (standard clauses, BCRs etc), or
- derogations or other specific circumstances apply (such as the explicit consent of the data subject)

➤ Breach notification

Controllers must notify the Commissioner of Data Protection if a breach compromises a data subject's confidentiality, security or privacy. If the risk to the data subject is high then the data subject must also be notified.

New accountability standards

► High Risk Processing Activities

Businesses in-scope will need to consider whether they conduct High Risk Processing Activities. If so, they must appoint a data protection officer. Data protection impact assessments must be conducted before a new High Risk Processing Activity is to occur. This is a new concept in DPL 2020.

A High Risk Processing Activity is:

- a processing that includes the adoption of new or different technologies or methods, which materially increases the risk to data subjects or renders it more difficult for data subjects to exercise their rights;
- b where 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, for example, on account of the sensitivity of the personal data or risks relating to the security, integrity or privacy of the personal data;
- c where the processing will involve a systematic and extensive evaluation

of personal aspects relating to natural persons, based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or

- d where a material amount of special categories of personal data are to be processed.

► Financial sanctions

Both controllers and processors may be subject to administrative fines of up to USD 100,000, and potentially unlimited fines for serious breaches, imposed by the Commissioner of Data Protection and both may also be liable under court order to pay compensation directly to data subjects. A processor is only liable for damage caused by processing where it has not complied with the obligations of the law specifically directed to processors, or where the processor has acted outside the lawful instructions of the controller. Where both a controller and a processor are liable for the infringing processing, their liability under the law is joint and several.

ACCOUNTABILITY



Distinct features of the DPL 2020

➤ Emerging tech and friction with GDPR

Processing methods are potentially subject to rapid change as technology develops. Data subject rights (such as the right of deletion) and principles (such as storage limitation) are potentially at odds with new processing methods (such as blockchain).

The DPL 2020 affords increased flexibility to controllers who wish to use such methods, but only if enhanced information provision obligations are complied with so that data subjects go into the relationship with full awareness and open eyes.

It is possible for controllers to refuse certain data subject rights if the relevant enhanced information provisions have been complied with.

➤ Non-discrimination

The DPL 2020 contains some non-discrimination provisions similar to those in the California Consumer Privacy Act. Data subjects cannot be discriminated against for exercising their rights.



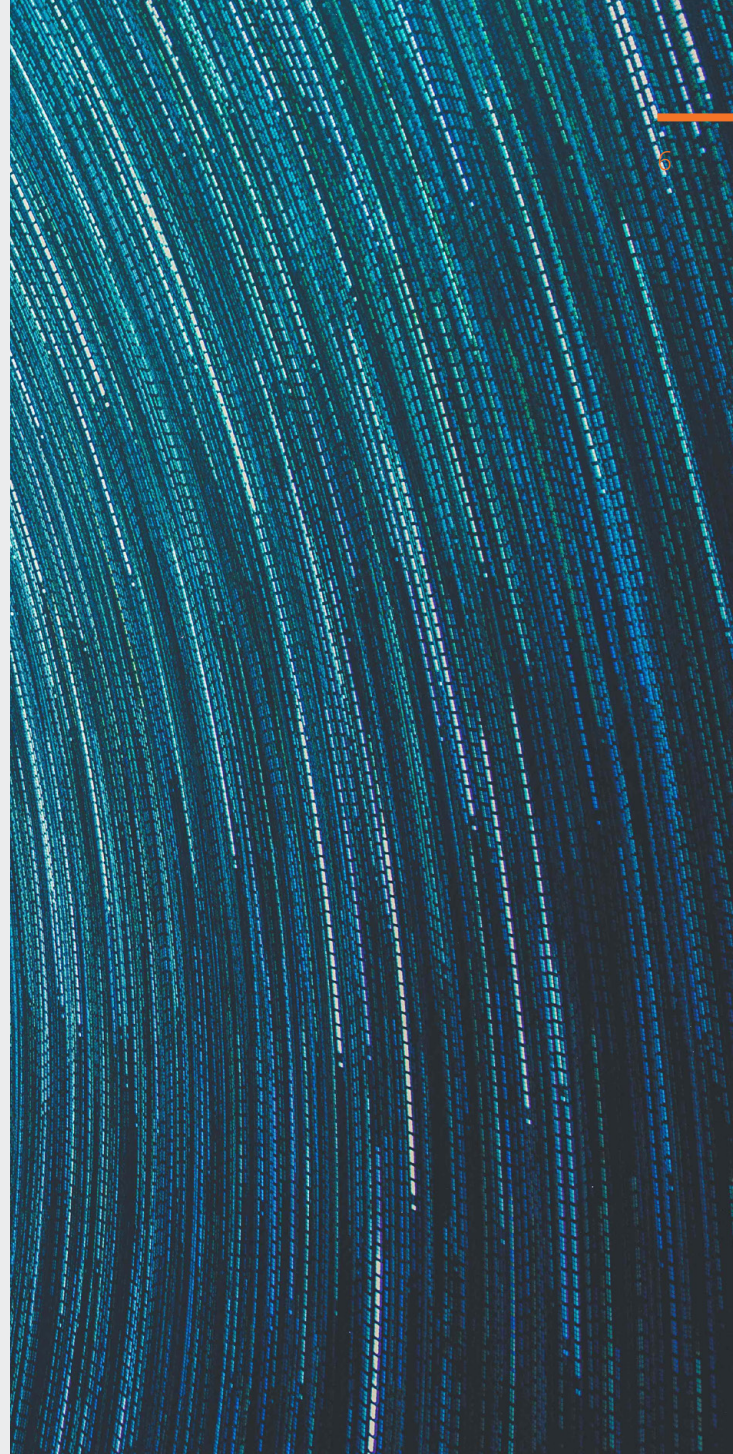
Readiness

Businesses which are already subject to the DIFC data protection law or to other regimes such as GDPR, should find that preparation for DPL 2020 is an evolutionary process, rather than a material upheaval. Nevertheless, DPL 2020 represents a significant increase in the depth and breadth of existing DIFC data protection law and it is important that organisations make adequate preparation for the law.

Clyde & Co has advised numerous businesses throughout the region on data protection matters and acted for the DIFC on the drafting of the new law.

We have also developed some standard data protection readiness packages for businesses.

For further details and information on DPL 2020, please [click here](#).



Contacts

Our TMT experts assist clients across a broad range of work including regulatory analysis and compliance, practical data protection issues, technology procurement and outsourcing, and market entry.



Dino Wilkinson
Partner
dino.wilkinson@clydeco.com



Ben Gibson
Senior Associate
ben.gibson@clydeco.com



Masha Ooijevaar
Associate
masha.ooijevaar@clydeco.com

440

Partners

1,800

Lawyers

4,000

Total staff

50+

Offices worldwide*

www.clydeco.com

*includes associated offices

Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority.

© Clyde & Co LLP 2020

1135797 – 05 – 2020