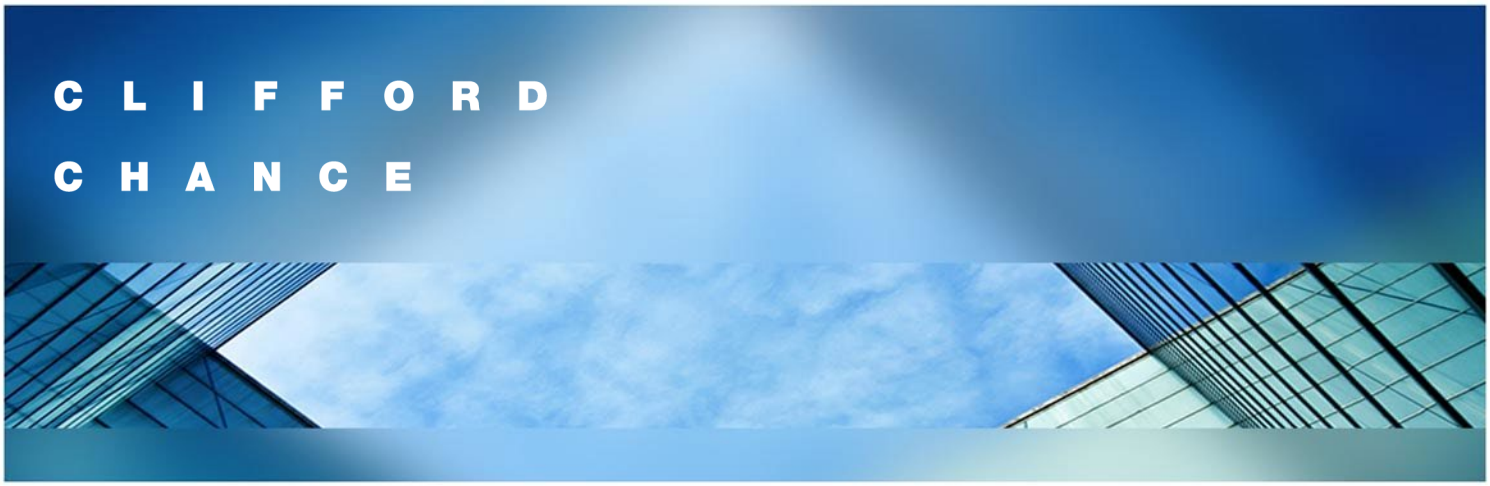

DATA PROTECTION IN THE UAE: A YEAR IN REVIEW

The UAE has seen some significant changes in the data protection landscape in the last 12 months which may soon culminate with the implementation of a new federal data protection law. In this briefing, Arun Visweswaran (Senior Associate) and Lana Ristic (Associate) look back at some of the key data protection developments in the UAE in the last year and practical tips for compliance.

Key issues

- In the last 12 months we have seen significant developments in the data protection landscape in the UAE.
- The DIFC has published guidance to assist business to comply with the DIFC Data Protection Law and has published standard contractual clauses for data transfers
- The ADGM Data Protection Regulations were enacted and align the ADGM with GDPR standards and requirements.
- The UAE Central Bank has established a Consumer Protection Framework to protect consumers of financial services (and their data).
- The data localisation requirements imposed by the UAE Health Data Law have been relaxed
- The implementation of the new UAE Data Protection Law remains imminent.

DIFC DATA PROTECTION LAW

It has now been more than a year since the DIFC Data Protection Law (the "**DIFC Law**") was enacted, and DIFC businesses should now be compliant with these data protection requirements.

To assist businesses with compliance, the DIFC has published guidance on a number of issues, such as: [1]

- notifications to the Data Commissioner in the event of a personal data breach;
- high risk processing guidance;
- data export guidance; and
- individuals' rights to access and control DIFC Personal Data.

For those businesses who have or are required to appoint a Data Protection Officer, the DIFC has published a checklist for Data Protection Officers when completing their annual Data Protection Controller Assessment.

The DIFC has also updated the standard contractual clauses for data transfers to jurisdictions that are not on the adequate jurisdictions list under the DIFC Law. The previous version of the DIFC standard clauses also remain valid until 27 December 2022 if the processing operations are unchanged. However, for new contracts, parties should use the updated clauses (which are in line with the updated EU standard clauses).

The DIFC has listed the UK as an adequate jurisdiction for data transfers following the completion of Brexit. In the same vein, the DIFC is engaging with the UK regulators with a view to being listed as an adequate jurisdiction by the UK.

1 The DIFC Data Protection guidance can be found here https://www.difc.ae/business/operating/data-protection/guidance/

ADGM DATA PROTECTION REGULATIONS

The ADGM enacted its new Data Protection Regulations 2021 (the "**ADGM Regulations**") in February 2021.

Like the DIFC Law, the ADGM Regulations reflect GDPR principles such as the appointment of Data Protection Officers, notifications of data breaches and the concept of high-risk processing activities.

Notably, the 2021 DP Regulations:

- Provide that the ADGM Regulations can apply to businesses outside the ADGM if the processing of personal data in the context of the activities of an ADGM occurs outside the ADGM;
- Provide revised grounds on which personal data may be transferred to other jurisdictions similar to the GDPR and the DIFC Law;
- Require notification of a data breach to be made within 72 hours of the controller becoming aware of the breach; and
- Grant the Commissioner the power to issued fines of up to USD 28 million for breaches of the 2021 DP Regulations.

Since the enactment of the ADGM Regulations, the ADGM Office of Data Protection has published:

- guidance on various aspects of the 2021 DP Regulations, such as data subjects' rights, international transfers and individuals' rights and remedies;[2]
- new rules on fees and fines; and
- standard contractual clauses – for both data transfers and agreements between data controllers and data processors (which is mandatory pursuant to Article 26 of the ADGM Regulations)

The ADGM Regulations provide a transition period of 12 months for existing establishments in the ADGM and 6 months for new establishments in the ADGM – both periods starting from the date of publication of the ADGM Regulations.

Both the DIFC Law and the ADGM Regulations adopt the concept of accountability from the GDPR where the onus is on businesses to conduct an analysis of their operations to determine which aspects of the relevant laws apply to them and then implement measures to comply. A failure to demonstrate compliance can have significant ramifications for businesses including, in the event of a cyber breach incident or an audit by the relevant data commissioners.

UAE CENTRAL BANK CONSUMER PROTECTION REGULATION AND RETAIL PAYMENT SERVICES REGULATION

Further to its consumer protection objectives, the UAE Central Bank issued the Consumer Protection Regulations in December 2020, followed shortly by

[2] The ADGM Data Protection guidance can be found here: https://www.adgm.com/operating-in-adgm/office-of-data-protection/guidance

the Consumer Protection Standards in January 2021 (together the "**Consumer Protection Framework**").

Together, these documents establish a framework for the protection of consumers of financial services, including the protection of the consumers' personal data.

The Consumer Protection Framework applies to all financial institutions licensed by the UAE Central Bank to carry out a Licensed Financial Activity ("**Licensed Financial Institutions**" or "**LFIs**") and who offer their products and services to consumers, which is defined as any natural person or sole proprietor who receives financial services or products (from an LFI), whether or not these services are paid for. They do not apply to financial freezone entities, for example, in the DIFC and ADGM.

In terms of data protection, the Consumer Protection Framework supplements the existing overriding confidentiality obligation on LFIs and represents a major development for data protection in onshore UAE as they resemble some of the data protection requirements found in the GDPR.

The key data protection features of the consumer protection framework include the requirements to:

- Establish a **data management** and protection function;
- Implement and maintain a **data retention policy**;
- **Minimise data collection** to only the extent required to carry out Licensed Financial Activities;
- Implement and maintain appropriate **security measures** to detect unauthorised access to data, **keep records** of unauthorised access and any harm caused;
- **Report** any significant data breaches to the Central Bank, and to affected consumers where the data breach may pose a risk to the consumer's financial or personal security;
- **Reimburse** the direct costs of actual harm suffered by consumers due to a data breach; and
- Ensure that consumers have the ability to make informed decisions regarding granting **consent** for the disclosure of their data to third parties.

Similarly, the UAE Central Bank's Retail Payment Services and Card Schemes Regulation ("**Retail Payment Regulations**") also imposes data protection obligations on entities providing retail payment services or operating card schemes in the UAE.[3] In particular, the Retail Payment Regulations:

- Require payment services providers to maintain adequate policies to protect personal and payment data.
- Provide that personal and payment data:
  - Must be processed and retained only with consent and to the extent that is necessary for the provision of the Retail Payment services.

[3] Circular No. 15/2021

  - May only be disclosed in limited circumstances, including to the subject, to the UAE Central Bank, other regulatory authorities (subject to the UAE Central Bank's consent) and third parties (subject to the user's consent).
  - Must be stored and maintained in the UAE.
- Require major security breaches, such as data leakage, to be reported to the UAE Central Bank.

LFIs and payment service providers regulated by the UAE Central Bank should therefore have in place appropriate systems to ensure compliance with the data protection requirements set out in these laws.

UAE HEALTH DATA LAW

Following the introduction of Federal Law No. 2 of 2019 (the "**Health Data Law**"), businesses in the health industry were subject to strict data localisation requirements which prevented health data related to healthcare services provided in the UAE from being transferred out of the UAE.

Pursuant to recent Ministerial Resolution 51 of 2021 (the "**Resolution**"), these data localisation requirements have been relaxed to some extent. The Resolution identifies a number of permitted exceptions to the Health Data Law's default prohibition on the transfer of health data out of the UAE. The permitted exceptions cover a broad array of health data and health services, such as data from scientific research, wearables and health care devices (e.g., smart watches), and telemedicine. It is worth noting that most of the permitted exceptions are still subject to some conditions. For example, there is a requirement to obtain approval from the relevant health authority in the case of transferring data arising from scientific research.

FEDERAL DATA PROTECTION LAW

While the implementation of the new UAE Data Protection Law is imminent, it is worth bearing in mind that there are a host of data protection requirements already in place in the UAE which adopt many GDPR concepts. It is anticipated that the new UAE Data Protection law would be based on some of the principles from these other laws. Therefore, businesses who are already compliant with such standards might find that the cost of compliance with the UAE Data Protection Law (once implemented) may not be that high compared to businesses who have not put in place a robust data protection and data management framework.

We have assisted various business with compliance measures with the existing laws and would be happy to discuss this further.

CLIFFORD
CHANCE

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

Lana Ristic
Associate

T 971 4503 2611
E lana.ristic
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Level 15, Burj Daman, Dubai International Financial Centre, P.O. Box 9380, Dubai, United Arab Emirates