UAE CORPORATE AND COMMERCIAL BITESIZE BULLETIN

ISSUE 2 – SEPTEMBER 2020

Marhaba and welcome to Issue 2 of the HFW UAE Corporate and Commercial Bitesize Bulletin.

In this issue we will be covering the recent changes to the data protection laws in the UAE.

In this Bulletin:

Data Protection

- Implementing Regulations for Health Data Law in the UAE issued
- DIFC issues new DIFC Data Protection Law

"The Health Data Law left several important matters to be further detailed in implementing regulations, including the controls and procedures for accessing the Central System and clarity on when health information and data relating to health services in the UAE may be stored, processed, generated or amended outside the UAE or the process by which an organisation may seek authorisation from the relevant health authority for such activity."

Implementing Regulations for Health Data Law in the UAE issued

In April 2020 the implementing regulations for Federal Law No. 2 of 2019 concerning the Use of the Information and Communication Technology (ICT) in the Health Sector (the Health Data Law) were issued by Cabinet Decision No. 32 of 2020 (the Implementing Regulations). The Health Data Law came into force in May 2019 and aims to regulate the use of ICT in the UAE healthcare sector.

Its objectives are to:

- ensure the optimal use of ICT in the healthcare sector;
- ensure compatibility with international standards and practices;
- to allow the Ministry of Health and Prevention (**Ministry**) to collect, analyse and retain health information and data; and
- to ensure the security and safety of health information and data.

The Health Data Law is the first federal legislation in the UAE that has a specific focus on data protection.

The Health Data Law applies to all entities in the UAE (including those in free zones) using ICT to process health information and data, including health care providers, insurance companies, brokers and third party administrators. "Health information" and "data" are very broadly defined and include any numbers, letters, codes and images which relate to health or insurance establishments or authorities, or to the beneficiaries of health services. Notably, there is no requirement for the health information or data to identify an individual.

Key aspects of the Health Data Law include:

- The establishment of a central IT system (the **Central System**) managed by the Ministry to store, process and exchange health information and data.
- The creation of data protection obligations adopting principles from international data protection laws, including confidentiality (subject to certain specific exemptions), accuracy, access and the adoption of security measures.
- A prohibition on storing, processing, generating or amending health information and data relating to health services provided in the UAE outside the UAE, unless authorised to do so by the relevant health authority in coordination with the Ministry.
- A requirement to retain health information and data for at least 25 years from the date of the last procedure.

The Health Data Law left several important matters to be further detailed in implementing regulations, including the controls and procedures for accessing the Central System and clarity on when health information and data relating to health services in the UAE may be stored, processed, generated or amended outside the UAE or the process by which an organisation may seek authorisation from the relevant health authority for such activity.

The Implementing Regulations come into force on 30 October 2020 and are heavily focussed on the controls and conditions for accessing the Central System. The Implementing Regulations do not provide any further details on the circumstances in which health information and data may be stored, processed, generated or amended outside the UAE which it likely to remain a key area of concern for those managing such information. The Implementing Regulations set out details relating to access to and use of the Central System further to Articles 7 and 8 of the Health Data Law, including:

- the rules for health authorities in relation to joining the Central System, in particular relating to access controls, audit and confidentiality;
- rights of the Ministry, in coordination with the federal or local health authorities to: (i) determine the mechanism and procedure for guaranteeing the quality of health information and data; and (ii) audit health information and data to verify their validity, quality and compliance; and

- the rules and conditions relating to the circulation and storage of health information and data, including a prohibition on disclosing health information and data without the patient's consent (except for in emergency circumstances) and a requirement for health information and data to be encrypted if it is sent by email or other electronic communication.

Notably, the Implementing Regulations give individuals the right to request that their health information is not accessed or that access is restricted. This right is to be exercised in accordance with conditions which are to be set by the Ministry in coordination with other health authorities. In addition individuals are also granted the right to opt-out of having their health information and data stored in the Central System.

Penalties for failure to comply with the requirements of the Health Data Law include suspension or withdrawal of the licence to use the Central System and fines of up to AED 1 million.

If your business is involved in the provision of services in or to the healthcare sector in the UAE, it is recommended that you review your current practices and ensure that you comply with the requirements of the Health Data Law and the Implementing Regulations.

DIFC issues new DIFC Data Protection Law

Following a public consultation in the summer of 2019, the DIFC enacted a new Data Protection Law (DIFC Law No. 5 of 2020) (the New Law) on 21 May 2020 to replace DIFC Law No. 7 of 2002 and the DIFC Data Protection Regulations (together the Previous Law).

The Previous Law was based on the European Data Protection Directive (Directive 96/EU/46/EC) which was superseded in May 2018 by the General Data Protection Regulation (**GDPR**) (Regulation (EU) 2016/679). The DIFC recognised the impact of the GDPR on business globally and the increasing number of jurisdictions that are enacting data protection laws which adopt many of the principles of the GDPR, including jurisdictions in the Middle East. To ensure consistency and familiarity for businesses in the DIFC, the New Law is, therefore, based on principles found in the GDPR, together with modifications to reflect the latest developments in technology, privacy and security law and the requirements of the DIFC. The DIFC has also issued the Data Protection Regulations 2020 (the **Regulations**) which provide additional detail on certain aspects of the New Law.

The New Law expands the scope of those that are subject to it. It applies to: (i) the processing of personal data by a controller or a processor incorporated in the DIFC, regardless of whether the processing takes place in the DIFC or not; and (ii) a controller or processor, regardless of its place of incorporation, that processes personal data in the DIFC as part of stable arrangements other than on an occasional basis, in the context of that processing. For the purposes of the New Law, "in the DIFC" means that the personnel used to conduct the processing are physically located in the DIFC. This means that companies registered onshore in the UAE may now be directly subject to the New Law.

Other key changes introduced by the New Law and Regulations are:

- Increased responsibility for processors, including an express obligation for processors to establish a program to demonstrate compliance with the New Law.
- The introduction of specific requirements in relation to obtaining consent for the processing of personal data and special categories of personal data.
- More comprehensive compliance obligations, including:
  - a requirement for controllers and processors to follow the principle of "data protection by design and default";
  - an express obligation for controllers and processors that collect or process personal data to implement and maintain an written data protection policy;
  - a requirement for controllers and processors to designate an independent data protection officer where they will be performing high risk processing activities on a systematic or regular basis; and
  - a requirement to complete data protection impact assessments where high risk processing activities are to take place.
- The introduction of new requirements for joint controllers and in relation to the appointment of processors, including requirements for written contracts between joint controllers and a legally binding contract between controllers and processors (and processors and sub-processors).
- The introduction of a principle of non-discrimination.
- Revised breach notification requirements and the introduction of a requirement to notify data subjects.
- The ability for the Commissioner (as the regulatory authority responsible for ensuring compliance with the New Law) to issue directions or warnings in the event of breach of the requirements of the New Law, in addition to imposing fines. A number of new fines have been introduced for specific breaches with fines ranging from USD10,000 to USD100,000. In addition, the Commissioner is granted the power to impose a general fine in an amount which is appropriate and proportionate. This general fine is not specifically calculated with reference to the turnover of the company or subject to an overall maximum limit.

The New Law and Regulations came into force on 1 July 2020, however, the DIFC has announced a transition period of three months until 1 October 2020, after which the New Law and Regulations will be enforced. Businesses established in the DIFC or which are processing personal data in the DIFC are advised to review their existing compliance programmes and to update them as necessary to ensure compliance with the enhanced requirements of the New Law and Regulations.

We hope you have enjoyed reading our update. If you have any questions, please do not hesitate to contact the authors of this article

TANIA DE SWART
Partner, Abu Dhabi
T +971 52 931 1118
E tania.deswart@hfw.com

JEMIMA MCDONALD
Senior Associate, Abu Dhabi
T +971 50 655 9340
E jemima.mcdonald@hfw.com

Research undertaken by Komal Fayyaz, Paralegal, Dubai

Alternatively please contact any of our Middle East Corporate Team.

RICHARD LUCAS
Partner, Abu Dhabi
T +971 56 333 7160
E richard.lucas@hfw.com

RULA DAJANI ABULJEBAIN
Partner, Dubai
T +971 50 6251285
E rula.dajaniabuljebain@hfw.com

VINCE GORDON
Partner, Abu Dhabi
T +971 50 622 1063
E vince.gordon@hfw.com

ALEX REID
Partner, Dubai
T +971 56 808 4031
E alexander.reid@hfw.com

JUSTIN WHELAN
Partner, Abu Dhabi
T +971 52 105 8439
E justin.whelan@hfw.com

JULIAN AWWAD
Senior Associate, Kuwait
T +965 9550 5688
E julian.awwad@hfw.com

ABEER GAROUSHA
Associate, Dubai
T +971 56 499 8397
E abeer.garousha@hfw.com

hfw.com

Americas | Europe | Middle East | Asia Pacific