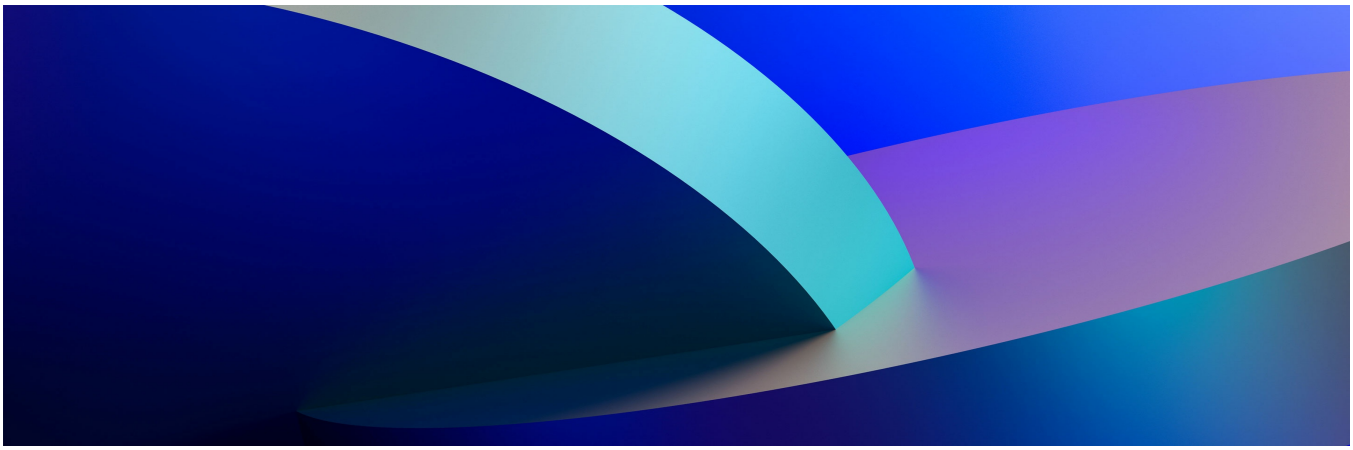

Data protection and cybersecurity laws in the United Arab Emirates

Data protection

1. Local data protection laws and scope

The UAE has a multi-layered legal system, with legislation issued at Federal and Emirate level. In addition, the UAE contains numerous special economic zones (**Free Zones**) which can pass their own legislation. In this paper, the UAE outside the Free Zones is referred to as **Onshore**. Where a Free Zone has not legislated for data protection, the relevant Onshore law will apply in this regard. All Onshore criminal law continues to apply in the Free Zones (whether such zones have a data protection law or not).

Federal Decree Law No. 45 of 2021 on the Protection of Personal Data ("**DPL**") applies to all processing of personal data Onshore. There are, in addition to the DPL, a number of sector and activity-specific laws with data protection aspects as well (which, in the case of the healthcare and banking sectors, take precedence over the DPL with respect to the activities in question). DPL took effect on 2 January 2022, however, it will not be enforced until 6 months after the publication of further implementing regulations. There is no published timeline for the publication of the executive regulations and at the time of writing they have not been published. Therefore, DPL is not currently being actively enforced. The DPL adopts similar concepts and approaches to the GDPR in many aspects, although there is no "legitimate interests" basis for processing personal data, which may lead to a heavier reliance on consent.

With respect to the Free Zones, the two special financial Free Zones – the Dubai International Financial Centre (**DIFC**) and the Abu Dhabi Global Market (**ADGM**) – each have data protection law modelled largely on GDPR. In addition, Dubai Healthcare City (**DHC**) has a data protection regulation which applies to patient medical information and is founded on similar principles.

Principal laws Onshore

- **DPL** – this applies to all personal data processing done by electronic means by any controller or processor located in the UAE (regardless of the location of the data subjects whose data are being processed) and any controller or processor located outside the UAE who processes the personal data of data subjects inside the UAE, subject to the following exceptions: i) the law confirms that it does not apply to companies and institutions located in Free Zones which have special data

protection legislation ; ii) the law does not apply to the government, the judiciary or security authorities or to « government data » ; iii) the law does not apply to processing in a domestic context; iv) the law does not apply with respect to health personal data subject to specific regulation ; v) the law does not apply to banking and credit data subject to specific regulation, The DPL will be managed and enforced by a national Data Office, established under Federal Law 44/2021.

- **the UAE Constitution** – this recognises a general concept of privacy for UAE citizens (i.e. Emirati nationals), in line with Shariah principles that recognise a right to privacy. UAE citizens only comprise a very small portion of the UAE population (less than 15% at the time of preparing this response).
- **Federal Law No. 3 of 1987 as amended (the Penal Code)** - Article 379 provides that it is a criminal offence for a person to disclose secret information relating to another person for his or her own gain without a lawful basis for doing so. A lawful basis can be understood to refer to a specific legal responsibility (such as responding to an official request) or to the consent of the data subject in question. The concept of "secret" is not defined and there is no system of binding precedent in UAE Onshore courts. This Article is likely intended to protect specific relationships of confidentiality (such as doctor/patient) and is more concerned with respect for an individual's private life and circumstances than with broader concepts relating to how data is collected and processed, nevertheless, entities collecting and disclosing personal data onshore are well-advised to consider obtaining clear consent to mitigate their risks. The Penal Code also criminalises illegal interception of correspondence and, under Article 378, it is an offence to intercept or eavesdrop on a private conversation or to capture or transmit images obtained of a person in a private place, in each case without the consent of the data subject.
- **Federal Decree-Law No. 5 of 2012 on Combatting Cybercrimes (Cybercrime Law) –** the law criminalises typical cybercrime acts such as hacking, unauthorised access to computer systems and information, amongst other things. The law also criminalises, under Article 21, the use of IT equipment or systems to invade the privacy of a person through publishing pictures, news or other information or by eavesdropping or intercepting their communications. If the consent of the individual has been obtained then this should be a defence to any complaint. Under Article 20 of the law it is an offence to use a computer network or IT system to insult a person or accuse them or a matter which shall cause them to be held in contempt. In practice, this law has been used to prosecute people for acts such as uploading content to social media without the permission of the subject in question or posting offensive remarks on social media about a person.
- **Federal Law No 2 of 2019 on the use of Information Technology in the Healthcare Sector** – this law requires all patient information relating to medical procedures carried out in the UAE to be kept secure and treated in accordance with good data protection principles. The law provides for the establishment of a centralised healthcare data system and for mandatory minimum retention periods of 25 years. Significantly, the law also prohibits the transfer of any such patient data outside the UAE without special permission from the relevant Emirate health regulator. In addition, the Abu Dhabi Department of Health has published detailed data standards under the law which are comprehensive and mandate a number of organisational and technical compliance steps to be undertaken (the law itself is rather high-level). It is likely that other Emirate health authorities will publish similar standards in due course.
- **Federal Law No 15 of 2020 on Consumer Protection (Consumer Protection Law)** is new UAE consumer protection legislation that was issued on 10 November 2020. The Consumer Protection Law establishes a right for consumers to have the privacy and security of their data protected and the right not to have it used for promotional and marketing purposes, however no detail in relation to how this right is exercised or managed in practice has been included. Please note that when a new Federal law is issued in the UAE this generally sets out broad principles of

how the law will apply and is subsequently supplemented by implementing regulations either at Emirate level or by the relevant competent authority. The implementing regulations for the Consumer Protection Law are yet to be published, so the specifics of how this law will apply are not yet known. Businesses have a one-year transition period (ie until November 2021) to ensure that they are complying with this legislation, which should provide sufficient time for the implementing regulations to be published and businesses to make any necessary changes.

- **Federal Law by Decree 3 of 2003 as amended (Telecoms Law)** includes the following implementing regulations/policies (Policies):
  - **Privacy of Consumer Information Policy (PCIP)**
  - **Consumer Complaint and Dispute Resolution Procedures**
  - **Consumer Complaint and Dispute Resolution Policy**
  - **Unsolicited Electronic Communications Regulatory Policy (Anti-SPAM Policy)**
  - **IoT Regulatory Policy (IoT Policy)**
  - The Telecommunications Law, including the PCIP, places an obligation on all telecommunications licensees to take measures to prevent the unauthorised use or disclosure of customer information stored electronically. The Anti-SPAM Policy requires Licensees to implement anti-spam measures and to block organisations sending excess unsolicited messages. The IoT Policy requires operators of IoT systems in the UAE to obtain appropriate licences from the TRA, to keep data processed by the system secure and not to transfer it outside the UAE. IoT Service Providers must adhere to the principles of purpose limitation, data minimisation and storage limitation.

- **Federal Regulatory Framework for Stored Values and Electronic Payment Systems of 2017** – digital payment service providers are required to keep personal data secure.

Principal Free Zone laws

- **DIFC and ADGM -** Both the DIFC and ADGM have recently enacted updated data protection laws/regulations to bring their legislation more closely into harmony with the GDPR. The DIFC issued Law No. 5 of 2020, the Data Protection Law (**DPL**), and accompanying Data Protection Regulations 2020, which was effective from 1 July 2020. The ADGM has issued Data Protection Regulations 2021 (**DPR**), which have recently come into effect. Both laws closely follow the principles of the GDPR and are based on concepts such as “data controller”, “data processor”, “personal data” etc. which are largely analogous to their GDPR equivalents. The bases on which personal data can be lawfully processed are also very similar to those found in the GDPR and data subjects are afforded very similar rights.
  - Unlike Onshore UAE, the DIFC and the ADGM both have specialist data protection regulators responsible for maintaining registers of controllers, proactively enforcing the law, providing guidance and consultation and liaising with other international data protection authorities.

- **Dubai Healthcare City** is a Free Zone focussed on healthcare services, which has its own regulations pertaining to the treatment of patient data by organisations licensed within the zone (DHA Health Data Protection Regulation, 2013) (**DHCR**). The regulations are based on similar principles and concepts to those found in the GDPR.

2. Data protection authority

UAE Onshore – Federal Decree Law No. 44 of 2021 Establishing the UAE Data Office (the **Data Office Law**) establishes the UAE Data Office as the regulator charged with overseeing, implementing and enforcing the DPL Onshore. The UAE Data Office is not yet operational. Responsibility for managing and enforcing sector-specific laws typically rests with the relevant ministry or authority – for example, in the case of onshore financial institutions, the UAE Central Bank is the licensing authority

and manages the Central Bank Consuler Protection Regulations which define data protection standards for the personal data of banking customers - and where the law is a general criminal law, with the police. Where the police are responsible for enforcement, they will investigate alleged breaches and determine whether the case should be referred to the public prosecutor's office which, in turn, will determine whether charges should be brought and whether a trial should commence.

DIFC – Commissioner of Data Protection.

ADGM – Data Protection Office.

Dubai Healthcare City – The Dubai Healthcare City Authority is responsible for implementing and enforcing all the Free Zone's laws and regulations. A Customer Protection Unit has been established by the authority and is responsible for dealing with complaints, and complaints made in relation to the DHCR are within its scope.

3. Anticipated changes to local laws

As mentioned above, we expect implementing regulations to the DPL to be published soon.

We also expect health authorities, such as the Dubai Health Authority, to follow a similar approach to that taken by the Abu Dhabi Department of Health and issue detailed patient data protection standards.

4. Sanctions & non-compliance

Administrative sanctions:

Onshore – the DPL does not contain details of the administrative sanctions that will apply but anticipates that the implementing regulations of the law will define the sanctions. There is no mention of any criminal sanctions in the DPL (but please note the potential overlap with the Cybercrime Law noted above). The DPL provides that data subjects may file a complaint with the UAE Data Office and that the UAE Data Office may subsequently impose an administrative penalty on offenders, but the DPL does not provide for an express right of compensation or redress in favour of the data subject. This may be clarified further in the executive regulations or data subjects may otherwise seek to have to bring claims based around tortious principles, rather than under clear statutory rights of redress.

Most of the other relevant laws are criminal laws but under Federal Law No 2 of 2019, violation can lead to a fine and/or suspension of access to the central health database. Violation of the TRA IoT Regulatory Policy is treated as a violation of the UAE's Telecommunications Law and could lead to administrative fines or the suspension of licences to carry on commercial activity.

DIFC – the maximum administrative fine that can be issued by the Commissioner of Data Protection for breach of the DPL or for breach of a direction issued by the Commissioner is USD 100,000. In addition, public reprimands may be issued. The Commissioner of Data Protection has the right to issue higher fines, without a specified limit for breaches of a serious non-administrative nature. Any person who receives an administrative penalty or direction has the right to seek judicial review in the courts of the DIFC.

ADGM – the maximum fine that can be issued by the Commissioner of Data Protection (the head of the Office of Data Protection) for breach of the DPR or for breach of a direction issued by the Commissioner is USD 28m. Any person who receives a fine or direction has the right to seek judicial review in the courts of the ADGM.

Dubai Healthcare City – the DHCR is not specific on the sanctions for breach but provides the authority with the ability to publish a list of penalties. This list does not seem to be readily publicly

available and may have been issued privately to licensees as a circular.

Criminal sanctions:

Violation of the Penal Code and the Cybercrimes Law can result in imprisonment for significant periods (for example, a prison sentence of at least six months for violating Articles 6 and 45 of the Cybercrimes Law) or significant fines. The revised Cybercrimes Law has only recently been published and come into effect, and there is no guidance or established practice as to how it will be enforced. The UAE Onshore legal system does not operate a binding system of court precedent, so there are no binding authorities which can be referred to, in order to determine how the Cybercrime Law would be applied. In practice, anecdotal reports tend to suggest that such provisions are invoked where the issue at hand is more concerned with invasion of privacy (betraying confidence, taking intrusive pictures/videos without permission, publicising private information) than with administrative or highly technical breaches of business-focused data laws, however there is no comprehensive public record to refer to in order to verify this.

The Consumer Protection Law provides for criminal sanctions in relation to certain breaches but is silent on the sanction for infringement of the provisions relating to use of customer data. The impending implementing regulations may clarify the position on such sanctions.

Others:

Under the DIFC and ADGM data protection laws, individuals have the right to seek damages if they suffer material or non-material harm as a result of an infringement.

Under the Onshore legal regime, an individual may have a tortious right to seek damages for harm suffered, in addition to filing a criminal complaint if applicable. The DHCR does not provide individuals with an express right to seek damages but does provide a right to raise a complaint and an individual may also be able to bring a tortious claim.

5. Registration / notification / authorisation

All business in the UAE are required to obtain an appropriate trade licence, either from the government when Onshore or the relevant free zone authority when in a free zone. There is no specific data processing registration, notification or authorisation requirement Onshore. However, the implementing regulations of the DPL which are yet to be published may detail such a requirement.

In DIFC and ADGM, entities subject to the data protection laws must register certain particulars relating to their processing activities.

6. Main obligations and processing requirements

Onshore - The DPL imposes similar requirements on controllers and processors as under the GDPR. Personal data must be processed pursuant to a legal basis and in accordance with data processing principles such as data minimization, transparency etc. Entities handling medical patient data, e-commerce businesses, consumer businesses, central-bank licensees and telecoms licensees (including provider of IoT services) are subject to various requirements to keep data secured and confidential but these are largely high-level requirements without associated demonstrable compliance obligations; the exception to the above is that businesses handling medical data in relation to Abu Dhabi-licensed medical procedures must comply with the detailed patient health data standard issued by the Department of Health, which contains a comprehensive list of compliance obligations, similar in many respects to those found in the GDPR. Strict localisation requirements apply to medical personal data.

In general, due to the risk of criminal complaint for invasion of privacy, businesses operating onshore wishing to adopt a prudent approach are well-advised to implement a process for obtaining

documented consent in relation to disclosure of personal information or any intrusive activity, particularly until an understanding of how the DPL will operate and be enforced is developed.

DIFC and ADGM – The principal data processing obligations are similar to GDPR, including that entities must: have a lawful basis for processing data; must process in accordance with principles such as purpose limitation; must provide information to data subjects when data is collected; must employ appropriate technical and organisational measures to protect data; must maintain a processing record; must be able to demonstrate compliance; must ensure processors are engaged under appropriate contractual terms; must respect data subject rights.

Dubai Healthcare City – the principles of the DHCR are similar to those found in the European Data Protection Directive, which predated the GDPR. Licensees must provide information to patients on the purposes for which their data are collected, must only use the data for such purposes, must keep it secure and must respect certain rights of the data subject.

7. Data subject rights

Onshore – The DPL introduces data subject rights similar to that afforded under GDPR subject to certain limitations. These rights include the right to be provided with processing information, the right to withdraw consent, the right to have incorrect data corrected, right to restriction of processing and a limited right of access to personal data. No timescales are provided for in which data subject requests must be complied with and no sanctions are specified for non-compliance. We assume that the implementing regulations of the law will address these matters. People receiving unwanted SPAM messages can also inform their telecoms service provider; telecoms licensees have an obligation to put in place measures to prevent unwanted SPAM and to block senders.

The Consumer Protection Law expresses that consumers have the right to have the privacy and security of their personal data protected and to not have their data used for promotional and marketing purposes but there is insufficient detail at this stage to determine what this means in practice.

DIFC and ADGM – data subjects have very similar rights to those afforded under the GDPR, such as the right to access their personal data, the right to object to certain processing, the right to portability in certain circumstances, the right not to be subject to automated decision making or profiling in certain circumstances, and the right to erasure in certain circumstances.

Dubai Healthcare City – under the DHCR, a patient has the right to confirmation as to the processing of his/her personal data, a right of access to the data and the right to have erroneous data corrected.

8. Processing by third parties

Onshore – The DPL does not specify mandatory provisions for inclusion in contracts between controllers and processors however data subjects need to be informed regarding the sectors or establishments with which the individual's personal data shall be shared.

DIFC and ADGM – any controller which engages a processor must ensure a written contract is in place that reflects various requirements of the data protection laws, similar to the GDPR.

Dubai Healthcare City – the DHCR does not prescribe specific controls or contractual requirements for third-party processors but makes it clear that the controller remains responsible for the data whilst it is processed by third parties. It is therefore incumbent on the controller to ensure appropriate contractual flow-downs.

9. Transfers out of country

Onshore – The DPL appears to adopt a permissive approach to personal data transfers. Personal data may be transferred outside of the UAE in various circumstances, including to countries which the UAE considers adequate for such purposes (details yet to be confirmed), pursuant to express data subject consent, where necessary to perform a contract with the data subject or to achieve the data subject's interests, and where there is a contract between the controller and the recipient which contains appropriate provisions.

Federal Law No 2 of 2019 prohibits the transfer of patient medical data out of the UAE without permission having been obtained from the relevant health authority.

The TRA IoT Regulatory Policy requires data processed in the context of IoT Services to be classified as Secret, Sensitive, Confidential or Open. All government data other than Open data must remain within the UAE. All Secret, Sensitive and Confidential data for individuals and businesses must be primarily kept within the UAE but may be transferred out of the UAE if the destination territory meets or exceeds the security and consumer protection standards upheld in the UAE (no further detail on which territories are considered adequate is provided). All personal data is considered "Secret" for these purposes.

Entities which are licensed by the UAE Central Bank are required to ensure that a copy of their banking data is retained in the UAE.

Government bodies will generally have a policy to keep data within the UAE, which may be more or less well codified from body to body.

DIFC and ADGM - Data flows from the DIFC and ADGM are controlled in a similar way to the GDPR, with certain territories considered to be adequate. Broadly, each of the zones recognises the other, plus the territories of the EEA and those that the EEA deems adequate, including the UK. It is important to note that Onshore UAE is not considered adequate. Transfers to non-adequate territories can be conducted provided additional safeguards or circumstances apply (such safeguards and circumstances being similar to those found in the GDPR).

Dubai Healthcare City – patient data can only be transferred out of DHC to a third party if an adequate level of protection for that patient data is ensured by the laws and regulations that are applicable to the third party and the transfer is either authorised by the patient or necessary for the ongoing provision of healthcare services to the patient. The DHCR provides that jurisdictions deemed adequate under the previous DIFC data protection law of 2007 are deemed adequate for the purposes of the DHCR. We are not aware of the DHCR having been updated in light of the new DPL 2020 in the DIFC but it seems likely that the list of adequate territories would be considered to match those deemed adequate by the DIFC from time to time, without the need for formal amendment.

10. Data Protection Officer

Onshore – The DPL requires a Data Protection Officer (**DPO**) to be appointed where processing involves: (a) a high-risk to the confidentiality and privacy of the personal data or data subject as a result of adopting technologies that are new or are associated with the volume of data in question ; (b) a systematic and comprehensive assessment of sensitive personal data, including profiling and automated processing ; or (c) processing involves a large amount of sensitive personal data. Where a DPO is not legally mandated, we recommend entities which handle personal data still ensure there is someone with senior status responsible for overseeing their data handling activities.

DIFC – the DIFC Data Protection Law 2020 includes the concept of High Risk Processing Activities. Any entity which performs High Risk Processing Activities systematically or regularly must appoint a Data Protection Officer (**DPO**), as must official DIFC bodies, other than the DIFC courts. The law defines the

required competency and status of the DPO. Details of the DPO must be provided to the Commissioner of Data Protection as part of the annual notification process (or sooner if the details are updated). The DPO should be based in the UAE, unless the entity is part of a broader group which has a group DPO capable of fulfilling the role and responsibilities. The DPO does not need to be an employee and can be engaged under a service contract.

ADGM – under the DPR, a DPO must be appointed by any public authority (other than the ADGM courts). Any other controller or processor subject to the law must appoint a DPO if their core activities consist of processing operations which require regular and systematic large scale monitoring of data subjects or consist of processing of special categories of personal data on a large scale. The DPR defines the position and tasks of the DPO. The DPO does not need to be based in the ADGM or the UAE. The identity of the DPO must be notified to the Commissioner of Data Protection. There is an exemption to the requirement to appoint a DPO if the entity in question has fewer than five employees, unless it is carrying out High Risk Processing Activities (as defined in the DPR, which is not directly equivalent to the same defined term in the DPL).

Dubai Healthcare City – the DHCR require each licensee to have an individual responsible for monitoring and ensuring compliance with the DHCR and dealing with requests made under the DHCR.

11. Security

Onshore – the DPL is not prescriptive as to specific data security standards that must be met, however both controllers and processors are responsible for establishing and taking appropriate technical and organisational measures to protect the data to a level commensurate with the risk.

A number of operational controls and security standards are specified in the Abu Dhabi Department of Health Patient Data Standard and Internet of Medical Things Security Standard. The TRA can mandate encryption standards that providers of Internet of Things services must adhere to.

DIFC and ADGM – there are obligations to keep personal data secure, which mandate a risk-based approach taking into account what is proportional and appropriate, similar to the GDPR.

Dubai Healthcare City – licensees must review and assess the security of their information systems and networks and make appropriate modifications to security policies, practices, measures and procedures on a regular basis and must periodically disclose security incidents to the DHCA's Consumer Protection Unit. Licensees must incorporate security as an essential element of information systems and networks.

12. Breach notification

Onshore – the DPL requires that controllers immediately notify the UAE Data Office and affected individuals of any infringement or breach of personal data which would prejudice the privacy, confidentiality and security of such data.

DIFC and ADGM – the data protection regulator should be notified of breaches as soon as practicable within the circumstances. Where the breach presents a high risk to the data subjects, the data subjects must also be notified, however there are some exceptions in the DPR that may apply to permit Controllers not to notify data subjects.

Dubai Healthcare City - the Consumer Protection Unit should be notified of security incidents.

13. Direct marketing

Onshore – The DPL does not detail the requirements for direct marketing, and it only specifies that data subjects have the right to object to and stop the processing of personal data where it is used for

direct marketing. Our understanding is that the express consent of the individual data subject is effectively required for direct marketing because there is no other processing basis that seems to be applicable; however, we hope the position will be clarified in the implementing regulations due to be published. We note the Consumer Protection Law says that suppliers should not use consumer data for direct marketing. We suspect that a blanket ban on direct marketing (which is widely used in the UAE) is not intended and that direct marketing will be possible, provided data subject consent has been obtained. As noted above, we hope the implementing regulations to the DPL will clarify this. Telecommunications licenses are required to seek to prevent SPAM phone calls and SMS messages and to block senders of excess SPAM.

DIFC and ADGM – direct marketing is not specifically regulated as an activity by the DPL or the DPR, although if data is to be used for direct marketing purposes then this must be specified in the processing information provided to data subjects. It is therefore up to the entity conducting the marketing to determine whether they have a lawful basis under the law to conduct the activity (for example, legitimate interests or consent). Data subjects have the right to object to their data being used for direct marketing purposes, and such objection should be respected.

Dubai Healthcare City – the DHCR does not expressly regulate direct marketing but provides that patient data should not be used for purposes contrary to the purpose of its collection, unless the patient has agreed to such use. Consent is therefore recommended if direct marketing to patients is to be carried out.

14. Cookies and adtech

Not specifically regulated Onshore or in the Free Zones (although social media advertising for medical purposes is regulated and all advertisements in any medium are subject to restrictions on content in line with the UAE's publication laws).

15. Risk scale

High (due to potential criminal sanctions, albeit general business obligations Onshore are not extensive)

16. Useful links

- DIFC Commissioner of Data Protection.: https://www.difc.ae/business/operating/data-protection/
- ADGM Data Protection Office: https://www.adgm.com/faqs/data-protection-office
- Abu Dhabi Department of Health standards: https://doh.gov.ae/en/resources/standards
- Dubai Healthcare City Regulations: https://dhcr.gov.ae/en/laws-and-regulations
- Telecommunications Regulatory Authority: https://www.tra.gov.ae/en/home.aspx
- UAE government cyber laws portal: https://u.ae/en/resources/laws

Cybersecurity

1. Local cybersecurity laws and scope

Federal Law

- Federal Decree Law No. 45 of 2021 on the Protection of Personal Data ("**DPL**")
- Federal Decree Law No. 34/2021 Cybercrime Law ('**Cybercrime Law**')
- UAE Cabinet Resolution No. 21 of 2013 regarding Information Security Regulation in Government Entities ('**Information Security Resolution**')
- UAE Federal Decree No. 11 of 2008 concerning the Human Resources in the Federal Government ('**HR Law**')

- UAE Penal Code (Federal Law 3 of 1987) ('**Penal Code**')
- UAE Electronic Transactions & E-Commerce Law (Federal Law 1 of 2006) ('**E-Commerce Law**')
- UAE Telecommunications Regulatory Authority Privacy of Consumer Information Policy ('**PCIP**')
- Federal Decree Number 3 of 2012 ('**Decree**')

Emirate-level Law

Dubai

- Dubai Law No. 2 of 2002 on Electronic Transactions and Commerce (**'Dubai E-Commerce Law**')

Abu Dhabi

- Abu Dhabi Government Information Security Standards Version 2.0 ('**Abu Dhabi Standards**')
- Abu Dhabi Government IT Architecture & Standards Framework ('**Abu Dhabi Framework**')
- Abu Dhabi Department of Health Patient Data Standard ('**Patient Data Standard**').

Government standards

There are also various government standards and policies which relate to data classification, data handling and storage, intra-governmental data sharing etc. and which apply only to government entities.

2. Anticipated changes to local laws

New laws are passed frequently in the UAE without public consultation or warning, so it is difficult to form a view as to the content of new laws that may be in the pipeline.

In November 2020, the UAE Cabinet agreed to establish the UAE Cybersecurity Council with the aim of developing a comprehensive cybersecurity strategy and creating a safe and strong cyber infrastructure in the UAE.

The council will be chaired by the Head of Cyber Security for the UAE Government and will contribute to creating a legal and regulatory framework that covers all types of cybercrimes, securing existing and emerging technologies and establishing a robust 'National Cyber Incident Response Plan' to enable swift and coordinated response to cyber incidents in the country.

We would expect, at some point, increasing documentation and definition of cybersecurity standards in sectors such as healthcare, critical infrastructure, banking and potentially cloud computing, although it is impossible to say with confidence when such laws may come into effect.

3. Application

The DPL applies to all personal data processing done by any controller or processor located in the UAE (regardless of the location of the data subjects whose data are being processed) and any controller or processor located outside the UAE who processes the personal data of data subjects inside the UAE. The law confirms that it does not apply to companies and institutions located in UAE free zones which have special data protection legislation and does not apply to businesses subject to specific data protection laws relating to health data and banking and credit data.

Information Security Resolution and the HR Law apply to UAE government entities only.

PCIP applies only to telecommunications licensees in the UAE, of which there are currently only two, both of which are owned by the UAE government.

Cybercrime Law, E-Commerce Law and Penal Code apply to anyone living or doing business in the UAE.

Dubai E-Commerce Law applies to anyone living or doing business in Dubai.

Abu Dhabi Government Standards apply to government entities in Abu Dhabi.

4. Authority

Federal Decree Law No. 44 of 2021 Establishing the UAE Data Office (the **Data Office Law**) establishes the UAE Data Office as the regulator charged with overseeing, implementing and enforcing the DPL Onshore. The UAE Data Office is not yet operational.

Ministry of Justice: Criminal sanctions under the Cybercrime Law, Penal Code and E-Commerce Law are applied after the public prosecution process has completed, so are ultimately enforced by the Ministry of Justice.

Federal Governmental Human Resources Authority: The Federal Governmental Human Resources Authority is responsible for enforcement of the HR Law.

Telecommunications Regulatory Authority (TRA): The TRA is responsible for enforcement of the PCIP.

Ministry of Justice and the Dubai Technology, Electronic Commerce and Media Free Zone Authority: Both the Ministry of Justice and the Dubai Technology, Electronic Commerce and Media Free Zone Authority are responsible for enforcement under the Dubai E-Commerce Law.

Chief Information Security Officers: The Abu Dhabi Security Standards are enforced by the Chief Information Security Officer in each Abu Dhabi government entity.

5. Key obligations

Federal Law

DPL is not prescriptive as to specific data security standards that must be met, however both controllers and processors are responsible for establishing and taking appropriate technical and organisational measures to protect the data to a level commensurate with the risk.

Cybercrime Law creates the criminal offences of accessing data without permission and transferring or disclosing confidential information without permission through an electronic system or IT tool. Although the Penal Code is not a cybersecurity mandate, it is the foundation for the idea in the UAE that personal information (to the extent it relates to an individual's private or family life) cannot be disclosed without the consent of the individual concerned.

Information Security Resolution establishes information security standards for all UAE federal entities and the employees working within them. It includes standards for email usage (including email usage on mobile phones), password creation, internet usage, anti-virus controls, information asset usage, desktop and laptop usage, encoding, back-up and copy control, WiFi security and data storage controls. It also classifies confidential information into different categories according to importance and/or sensitivity.

HR Law confers an obligation on federal entities to protect electronic confidential information relating to their employees and also imposes an obligation on civil servants to return all electronic files containing Ministry information at the end of their employment.

The **Penal Code** criminalises the use of a device to intercept or eavesdrop on a private communication.

E-Commerce Law incentivises the use of security authentication procedures. It states that all records, documents and signatures relating to electronic transactions and commerce that are subject

to a secure authentication procedure (to verify the identity of the sender) are deemed to create a secure electronic record of that transaction or communication.

PCIP places an obligation on all telecommunications licensees to take measures to prevent the unauthorised use or disclosure of customer information stored electronically. The PCIP does not specify the relevant measures that have to be taken. However, best practice would be to take appropriate technical security measures against unauthorised or unlawful processing of, and against accidental disclosure of, personal data. The measures taken must ensure a level of security that is sufficiently adequate to minimise the risk of liability arising out of a claim for breach of privacy made by a data subject.

Decree establishes a federal body for cyber security called the National Electronic Security Authority. In accordance with Article 5 of the Decree, the Authority is responsible for the design, national coordination and enforcement of the UAE's cyber security policies and legislation. The creation of a national electronic security authority demonstrates the growing importance of cyber security in the UAE.

Emirate-level Law

Dubai

- **Dubai E-Commerce Law** reiterates the federal E-Commerce Law, but at an Emirate government level.

Abu Dhabi

- **Abu Dhabi Standards** impose security standards on all Abu Dhabi Government personnel and contractors, as well as third parties handling Abu Dhabi Government data. The standards relate to 51 control objectives that serve to identify the unique targets states for each of the 14 policies. These objectives constitute the major initiatives of the Information Security Programme, and the standards are aligned with ISO 27002.
- **Abu Dhabi Framework** contains security principles for IT architecture established for and by the Abu Dhabi Government, including considering security at all levels of IT architecture and controlling access.
- The **Patient Data Standard** imposes a number of operational security requirements on entities licensed to carry out medical services in Abu Dhabi (which such entities must also ensure their suppliers and other contractors comply with). The standard is issued pursuant to Federal Law No 2 of 2019, which imposes obligations of security on patient data in high-level terms, including an obligation for all patient personal data to be kept within the UAE.

6. Sanctions & non-compliance

DPL

The DPL does not contain any administrative or criminal penalties for breaches of its laws however we expect that this will be dealt with by the implementing regulations due to be published.

Cyber Crimes Law and Penal Code

The police in each Emirate have developed specialised cybercrime units to handle complaints that relate to breaches of the cybercrime law and related offences. The cybercrime unit in the Emirate where the offender resides or where the disclosure occurred will have jurisdiction over a data subject's complaint.

The cybercrime unit would investigate the case and decide whether to refer it to the Public Prosecutor

in the same Emirate. If the case is referred and the Public Prosecutor is satisfied with the findings of the cybercrime unit, charges would be brought against the suspect and heard in the courts.

Punishments under the Cyber Crime Law range from temporary detention, a minimum prison sentence of between six months or one year and/or a fine between AED 150,000 and AED 1m (Articles 2, 3, 7, 21 and 22 of the Cyber Crime Law). If found guilty of an attempt to commit any of the relevant offences under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 40).

The Penal Code would also be enforced in the same manner described above and, depending on the nature of the complaint, a specialist police unit may be involved in investigating the alleged offence.

Telecommunications Law

The TRA is responsible for overseeing the enforcement of the PCIP (and all telecommunications regulation in the UAE). Where a licensed telecommunications service provider has breached the Law, the subscriber/data subject generally needs to complain first to the service provider about the breach (Clause 3.1 Consumer Complaint and Dispute Procedure), though a direct approach to the TRA may be possible (Clause 4.1 of the Consumer Complaint and Dispute Resolution Policy). The subscriber may complain to the TRA if the breach is not satisfactorily resolved within thirty days as of the date of the complaint (Clause 2.2.1 Consumer Complaint and Dispute Procedure) or a longer period if the service provider notifies the subscriber of this extended period (Clause 2.2.1 Consumer Complaint and Dispute Procedure).

The subscriber's complaint needs to be submitted to the TRA within three months of the date when the service provider last took action (Clause 3.2 Consumer Complaint and Dispute Procedure). This three-month requirement may be waived subject to the discretion of the TRA (Clause 3.3 Consumer Complaint and Dispute Procedure).

After examining the complaint, the TRA may direct the service provider "to undertake any remedy deemed appropriate".

Federal Law No 2 of 2019 – Healthcare

Sanctions for failing to handle patient medical data in accordance with the law include a fine of up to AED 1m and the possible blocking of access to the central healthcare information system. Loss of such access could render it virtually impossible for a healthcare provider to carry on their business lawfully, so is a very serious sanction.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

No – but this is a stated aim of the creation of the UAE Cybersecurity Council in November 2020

8. National cybersecurity incident management structure

No – but this is a stated aim of the creation of the UAE Cybersecurity Council in November 2020

9. Other cybersecurity initiatives

As noted above, the UAE Cybersecurity Council was created in November 2020, so we expect various initiatives to be implemented over the short and medium term.

10. Useful links

- Telecommunications Regulatory Authority: https://www.tra.gov.ae/en/home.aspx
- UAE government cyber laws portal: https://u.ae/en/resources/laws

- UAE government cyber safety webpage: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

Key Contacts

Ben Gibson
Dubai
Partner

Authors

Ben Gibson
Dubai
Partner

Victoria Noto
Senior Associate
left_cms

Kate Corcoran
Dubai
Senior Associate