DATA PROTECTION LAWS OF THE WORLD

UAE - General

UAE - GENERAL

Last modified 18 January 2024

LAW

Note: Please also see UAE – Dubai (DIFC), UAE – ADGM, UAE – DHCC.

Generally

As part of the 50th anniversary of its founding, the United Arab Emirates (“**UAE**”) has issued a set of sweeping legal reforms, including the much anticipated Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data Protection (“**PDPL**”), which was issued on 26 September 2021.

The executive regulations to the PDPL (“**Executive Regulations**”) were due to be published within six months of the issuance of the PDPL. However as of 31 December 2023, those have not yet been published. Once the Executive Regulations are issued, organisations have a further six months from their date of the issuance in which they can adjust operations to compliance with the PDPL.

Reassuringly, the PDPL does not contain any major divergences from other well-known data protection regimes, including the GDPR. In this regard we expect it will be welcomed by local, regional and international businesses, in particular those that rely heavily upon personal data and international personal data flows. International businesses with global privacy compliance programs should seek to expand those to cover the UAE and achieve some synergies. However, businesses that are not used to compliance with laws like the GDPR may find some of the new obligations challenging; for example, the PDPL introduces rights for individuals to access, rectify, correct, delete, restrict processing, request cessation of processing or transfer of data, and object to automated processing. There are also new requirements around transfers of data outside of the UAE and requirements to keep data secure, and to notify the new data protection regulator, and in some circumstances Data Subjects, of data breaches. The requirements regarding keeping data secure, and new data breach obligations, will definitely up the ante for businesses in the UAE to take cyber security seriously.

Territorial Scope

The PDPL applies to:

- processing of personal data of people residing in the UAE, or people having a business within the UAE;
- each Controller or Processor inside the UAE, irrespective of whether the personal data they process is of individuals inside or outside the UAE
- each Controller or Processor located outside the UAE, who carries out processing activities of Data Subjects that are inside the UAE.

Other data protection and privacy laws in the UAE

The PDPL keeps intact existing data protection and privacy laws within the UAE’s financial free zones, DIFC and ADGM, as well as the rules of the Dubai Health Care City, (links to our summaries are above) as well as applicable onshore laws regulating health data and banking and credit data. For this reason the data protection landscape in the UAE (and the wider GCC region) remains complex to navigate and somewhat fragmented, meaning that the application of the PDPL will need to be considered carefully.

There are several UAE federal level laws that contain various provisions in relation to privacy and the protection of personal data:

- United Arab Emirates Constitution of 1971;
- Federal Law 31 of 2021, on the Issuance of the Crimes and Penalties Law (“UAE Criminal Law”);
- Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes (“UAE Cyber Crime Law”);
- Federal Law by Decree No. 3 of 2003 as amended) On Organising the Telecommunications Sector (“UAE Telecommunications Law”) including several implementing regulations / policies enacted by the Telecommunications and Digital Government Regulatory Authority ('TDRA') in respect of data protection of telecoms consumers in the UAE.

There are also some federal level sectoral regulations in banking and finance, and in health, which should be considered.

The Central Bank Law (Federal Law No. 14 of 2018); Central Bank’s Consumer Protection Regulation issued under Central Bank Notice No. 444 of 2021, and related Central Bank Consumer Protection Standards issued under Notice No. 1158 of 2021 on Consumer Protection Standards

Article 120 of the Central Bank Law requires that all data and information related to customers should be considered confidential in nature.

On 31 December 2020 the UAE Central Bank published its Consumer Protection Regulation. It applies to all Central Bank Licensed Financial Institutions, which had one year in which to ensure their compliance.

Article 6 of the Consumer Protection Regulation requires that Licensed Financial Institutions must collect the minimal amount of Consumer Data and information needed in respect of their licensed activities and remain in compliance with all other related laws and treat Consumers' information relationships and business affairs as private and confidential.

The Central Bank Consumer Protection Standards outline detailed requirements regarding how Licensed Financial Institutions must comply with. These standards include Licensed Financial Institutions:

- having a proper Data Management Control Framework;
- using secure digital transaction processing and controls;
- designating responsibility and accountability for the data management and protection function to a senior position in management who reports directly to senior management;
- ensuring personal data is:
    - collected for a lawful urpose directly related to the Licensed Financial Activities of the Licensed Financial Institution;
    - adequate and not excessive in relation to the stated purpose; and
    - collected with appropriate security and protection measures against unauthorized or unlawful processing and accidental loss, destruction, or damage.
- notifying consumers prior to requesting consent to share consumer personal data;
- obtaining express consent of consumers prior to use or sharing of their data;
- retaining all personal data, documents, records and files securely for a minimum of 5 years;
- notifying the Central Bank of any material data breaches, losses, destruction or alteration when they occur.

Central Bank’s Stored Value Facilities Regulation

On 30 September 2020 the UAE Central Bank issued a new Stored Value Facilities Regulation (“SVF Regulation”), repealing and replacing the Regulatory Framework for Stored Values and Electronic Payment Systems it has issued in September

2016. While the SVF Regulation makes amendments to the licensing and enforcement regime for SVF (on onshore UAE only; it does not apply in, or affect, the DIFC and ADGM free zones), from a data protection perspective little has changed. The SVF Regulation applies to those providing Stored Value Facilities, which is now defined as “*a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the “Relevant Undertaking”. SVF includes Device-based Stored Value Facility and Non-device based Stored Value Facility”*.

Article 10 of the SVF Regulation requires that licensees providing SVF services (**“SVFLicensee**”) must have in place adequate policies, measures and procedures to protect its information and accounting systems, databases, books and accounts, and other records and documents from unauthorized access, unauthorized retrieval, tampering and misuse.

An SVF Licensee must also adequately protect customer data (including customer identification and transaction records) which are required to be stored and maintained in the UAE. Such data can only be made available to the corresponding customer, the Central Bank, other regulatory authorities following prior approval of the Central Bank, or by a UAE court order. An SVF Licensee must store and retain all customer and transaction data for a period of five years from the date of the creation of the customer data, or longer if required by other laws.

Article 8 of the SVF Regulation requires that outsourcing arrangements must also contain adequate data protection and data handling controls.

Central Bank’s Retail Payment Services and Card Schemes Regulation

On 6 June 2021, the UAE Central Bank issued the Retail Payment Services and Card Schemes[1] Regulation (“Retail Services Regulation”). The Retail Services Regulation outline obligations and controls for the provision of Retail Payment Services and Card Schemes.

A Retail Payment Service includes any of the following: Payment Account Issuance Services; Payment Instrument Issuance Services; Merchant Acquiring Services; Payment Aggregation Services; Domestic Fund Transfer Services; Cross-border Fund Transfer Services; Payment Token Services; Payment Initiation Services; and Payment Account Information Services. The Retail Services Regulation does not apply to Stored Value Facilities.

Article 10 of the Retail Services Regulation requires that Payment Service Providers must have in place adequate policies, measures and procedures in relation to corporate governance, risk management, accounting and audit, record keeping, notification requirements and professional indemnity insurance. Amongst other things, article 10 requires the maintenance of confidential information, and that Payment Service Providers keep all necessary records on Personal and Payment Data for a period of 5 years.

Payment Service Providers must also put in place measures to ensure all business records can be restored in case they are lost, and that Retail Payment Service Users can access their own records in a timely manner. Payment Service Providers are also obligated to notify users of any loss in their records, and make reasonable effort to ensure that personal records are not wrongfully used.

Article 14 covers obligations towards Retail Payment Service Users, including protection of payment and personal data. Payment Service Providers to put in place policies and procedures to protect payment data and personal data and that Payment Service Providers only disclose Payment and Personal Data under the conditions outlined in the article.

The Retail Services Regulation further requires that Payment Service Providers store and maintain personal and payment data within the UAE, and must establish a safe and secure backup of all Personal and Payment Data in a separate location for the required period of 5 years.

Article 18 of the Retail Services Regulation considers Card Schemes, and place obligations on Card Scheme’s to notify the Central Bank in the case of a Data Breach no later than 72 hours after having become aware of such Data Breach.

ICT in Health Fields Law and Regulations, and Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the State

On 6 February 2018 Federal Law No. 2 of 2018 on the Use of the Information and Communication Technology (“**ICT ”) in Health Fields (“**ICT in Health Fields Law**”) was issued. The primary purpose of the ICT in Health Fields Law is to establish a central electronic system of medical records for use within the health industry within the UAE.

Article 13 of the ICT in Health Fields Law states that the Health Information and data related to the health services provided in the UAE may not be stored, processed, generated or transferred outside the UAE, unless in the cases defined by virtue of a decision issued by the Health Authority of the relevant emirate in coordination with the Federal Ministry of Health.

The Minister of Health issued a decision on 28 April 2021 outlining the circumstances when Health Information can be transferred outside of the UAE.

The UAE ICT in Health Fields Law applies to all Competent Entities.

“Competent Entity” is defined as "*Any entity in the State providing medical services, health insurance or national health insurance services, brokerage services, claims management services or electronic services in the medical field of any entity related, whether directly or indirectly, to the implementation of the provisions hereof.*"

“Health Information” is defined as *“The health information that were processed and were given a visual, audible or readable indication, and that may be attributed to the health sector, whether related to the health or insurance facilities or entities or to the health services beneficiaries.”*

On 22 April 2020 the Federal Cabinet issued Cabinet Resolution No. 32 of 2020 concerning the Regulations Concerning the Use of the Information and Communications Technology in the Areas of Health (“**ICT in Health Fields Regulation s”). The regulations provide further details, including on permission controls to access and use the central system, and on the storage and exchange of information on the central system.

Dubai Data Law

In December 2015 the Dubai Government published the Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, ("**Dubai Data Law**"). The purpose of the Dubai Data Law to collate and manage data that relates to the emirate of Dubai and, where appropriate, to publish it as “Open Data” or at least ensure that it is shared it between authorised persons. This law is considered unique as it is the only one in the world we are aware of that provides a government with the power to require designated private sector entities to provide to a government with information held by the company in relation to a city, for the purposes of making that information Open Data.

1: The Retail Services Regulation define Card Schemes as “*a single set of rules, practices and standards that enable a holder of a Payment Instrument to effect the execution of Card-based Payment Transactions within the State which is separated from any infrastructure of payment system that supports its operation, and includes the Card Scheme Governing Body. For the avoidance of doubt, a Card Scheme may be operated by a private or Public Sector Entity*”.

DEFINITIONS

The PDPL contains the following definitions.

Definition of Personal Data

“Personal Data” is defined as any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking data, using identifiers such as name, voice, picture, identification number, online identifier, geographic location, or one or more special features that express the physical, psychological, economic, cultural or social identity of such person. It also includes Sensitive Personal Data and Biometric Data.

Definition of Sensitive Personal Data

“Sensitive Personal Data” is defined as any data that directly or indirectly reveals a natural person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data, or any data related to the health of such person, such as his / her physical, psychological, mental, genetic or sexual condition, including information related to health care services provided thereto that reveals his / her health status.

Definition ofBiometric Data

“Biometric Data” is defined as Personal Data resulting from Processing, using a specific technique, relating to the physical, physiological or behavioral characteristics of a Data Subject, which allows or confirms the unique identification of the Data Subject, such as facial images or dactyloscopic data.

Definition of Processing

“Processing” is defined as any operation or set of operations which is performed on Personal Data using any electronic means, including Processing and other means. This process includes collection, storage, recording, organization, adaptation, alteration, circulation, modification, retrieval, exchange, sharing, use, or classification or disclosure of Personal Data by transmission, dissemination or distribution, or otherwise making it available, or aligning, combining, restricting, blocking, erasing or destroying Personal Data or creating models therefor.

Definition of Automated Processing

“Automated Processing” is defined as Processing that is carried out using an electronic program or system that is automatically operated, either completely independently without any human intervention, or partially independently with limited human supervision and intervention.

Definition of Controller

“Controller” is defined as an establishment or natural person who has Personal Data and who, given the nature of his / her activity, specifies the method, criteria and purpose of Processing such Personal Data, whether individually or jointly with other persons or establishments.

Definition of Processor

“Processor” is defined as an establishment or natural person who processes Personal Data on behalf of the Controller, as directed and instructed by the Controller.

Definition of Data Subject

“Data Subject” is defined as The natural person who is the subject of the Personal Data.

NATIONAL DATA PROTECTION AUTHORITY

At the date of writing this update the Data Office responsible for administering and enforcing the PDPL has not yet been established.

The UAE Central Bank is responsible for its Consumer Protection Regulation and Standards, the SVF Regulation and the Retail Services Regulation.

The Ministry of Health and Prevention is responsible for the ICT in Health Fields Law.

The Telecommunications and Digital Government Regulatory Authority (“**TDRA**”) is responsible for the regulation of its Consumer Protection Regulations.

REGISTRATION

There are no data protection registration requirements in the PDPL.

DATA PROTECTION OFFICERS

Processors and Controllers who are:

- conducting data processing which would cause a high risk to the confidentiality and privacy of the Data Subject’s personal data as a consequence of adopting new or data size-based technologies;
- conducting data processing will involve a systematic and comprehensive assessment of sensitive personal data, including profiling and automated processing; or
- processing large volumes of sensitive personal data will be processed,

will need to appoint a DPO.

The DPO can be a staff member or someone working on a service contract and does not necessarily need to be located in the UAE.

COLLECTION & PROCESSING

Data Protection Controls (Article 5)

Under the PDPL, Personal Data must be processed according to the following controls:

- Processing must be made in a fair, transparent and lawful manner;
- Personal Data must be collected for a specific and clear purpose, and may not be processed at any subsequent time in a manner incompatible with that purpose. However, Personal Data may be processed if the purpose of Processing is similar or close to the purpose for which such data is collected;
- Personal Data must be sufficient for and limited to the purpose for which the Processing is made;
- Personal Data must be accurate and correct and must be updated whenever necessary;
- Appropriate measures and procedures must be in place to ensure erasure or correction of incorrect Personal Data;
- Personal Data must be kept securely and protected from any breach, infringement, or illegal or unauthorized Processing by establishing and applying appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard;
- Personal Data may not be kept after fulfilling the purpose of Processing thereof. It may only be kept in the event that the identity of the Data Subject is anonymized using the “Anonymization” feature;
- Any other controls set by the Executive Regulations of this Decree Law.

Legal Bases for Processing (Article 4)

The PDPL prohibits Processing Personal Data without the consent of the Data Subject, except in the following cases:

- if the Processing is necessary for the Controller or Data Subject to fulfill his / her obligations and exercise his / her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws;
- if the Processing is necessary to perform a contract to which the Data Subject is a party or to take, at the request of the Data Subject, procedures for concluding, amending or terminating a contract;
- if the Processing is necessary to protect the interests of the Data Subject;
- if the Processing is for Personal Data that has become available and known to the public by an act of the Data Subject;
- if the Processing is necessary to protect the public interest;
- if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures;

- if the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the State;
- if the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the State;
- if the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the State;
- if the Processing is necessary to fulfill obligations imposed by other laws of the State on Controllers;
- any other cases set by the Executive Regulations.

Processing of Sensitive Personal Data

Unlike the GDPR, the PDPL does not impose more stringent controls around processing of Sensitive Personal Data, however if a Controller or Processor is Processing that involves a systematic and comprehensive assessment of Sensitive Personal Data, including profiling and automated processing, or if the Processing will be made on a large amount of Sensitive Personal Data, then the Controller or Processor must appoint a Data Protection Officer (Article 10).

Article 21 also requires that DPIAs be conducted before Processing that will use any of the modern technologies that would pose a high risk to the privacy and confidentiality of the Personal Data of the Data Subject, if the Processing will be made on a large amount of Sensitive Personal Data (Article 21)

Transparency (Privacy Notices)

The PDPL contains a broad obligation to process personal data in a transparent manner. This obligation is not placed specifically on either Controllers or Processors, so it can be assumed that it is intended to apply to both. Under other data protection laws, the general transparency obligation is often tied to a clear obligation to provide a privacy notice to Data Subjects which meets prescriptive content requirements. The PDPL does (yet) not have an express provision regarding this (although it is possible that the Executive Regulations may do). However, the PDPL does give Data Subjects a detailed right of access (without charge) to the types of information which would ordinarily be contained in a privacy notice. Moreover, per Article 13 of the PDPL, the Controller is required to, in all cases and prior to the commencement of processing, provide Data Subjects with information regarding:

- the purposes of the processing;
- the targeted sectors or establishments with whom the personal data will be shared, both within and outside the UAE; and
- the protection measures for cross-border processing.

Therefore, in practice, Controllers may ultimately consider publishing privacy notices that contain, at least in broad terms, the information that the Data Subject is entitled to seek under the PDPL.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data replicating those in the EU GDPR. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right to obtain information (‘data access’) (Article 13)

A Data Subject is entitled to request access to and obtain the following information without charge:

- the types of his / her Personal Data that is processed;
- purposes of Processing;
- decisions made based on Automated Processing, including Profiling;
- targeted sectors or establishments with which his / her Personal Data is to be shared, whether inside or outside the State;
- controls and standards for the periods of storing and keeping his / her Personal Data;

- procedures for correcting, erasing or limiting the Processing and objection to his / her personal data;
- protection measures for Cross-Border Processing;
- procedures to be taken in the event of a breach or infringement of his / her Personal Data, especially if the breach or infringement poses a direct and serious threat to the privacy and confidentiality of his / her Personal Data;
- the process of filing complaints with the Data Office.

Right to request Personal Data transfer (‘data portability’) (Article 14)

The Data Subject has the right to obtain his / her Personal Data provided to the Controller for Processing in a structured and machine-readable manner, so long as the Processing is based on the Consent of the Data Subject or is necessary for the fulfillment of a contractual obligation and is made by automated means.

The Data Subject has the right to request the transfer of his / her Personal Data to another Controller whenever this is technically feasible.

Right to correction or erasure ('right to be forgotten') (Article 15)

The Data Subject has the right to request the correction or completion of his / her inaccurate Personal Data held with the Controller, and has the right to request the erasure of his / her Personal Data held with the Controller in any of the following cases:

- if his / her Personal Data is no longer required for the purposes for which it is collected or processed;
- if the Data Subject withdraws his / her Consent on which the Processing is based;
- if the Data Subject objects to the Processing or if there are no legitimate reasons for the Controller to continue the Processing;
- if his / her Personal Data is processed in violation of the provisions hereof and the legislation in force, and the erasure process is necessary to comply with the applicable legislation and approved standards in this regard.

Right to restriction of Processing (Article 16)

The Data Subject has the right to oblige the Controller to restrict and stop Processing in any of the following cases:

- if the Data Subject objects to the accuracy of his / her Personal Data, in which case the Processing shall be restricted to a specific period allowing the Controller to verify accuracy of the data;
- if the Data Subject objects to the Processing of his / her Personal Data in violation of the agreed purposes;
- if the Processing is made in violation of the provisions hereof and the legislation in force.

The Data Subject has the right to request the Controller to continue to keep his / her Personal Data after fulfillment of the purposes of Processing, if such data is necessary to complete procedures related to claiming or defending rights and legal proceedings.

Right to stop Processing (Article 17)

The Data Subject has the right to object to and stop the Processing of his / her Personal Data in any of the following cases:

- if the Processing is for direct marketing purposes, including Profiling related to direct marketing;
- if the Processing is for the purposes of conducting statistical surveys, unless the Processing is necessary to achieve the public interest;
- if the Processing is in violation the controls referred to in Article 5 (referred to above)

The right not to be subject to automated decision making, including profiling (Article 18)

The Data Subject has the right to object to decisions issued with respect to Automated Processing that have legal consequences or seriously affect the Data Subject, including Profiling. However, the Data Subject may not object to the decisions issued with respect to Automated Processing in the following cases:

- if the Automated Processing is included in the terms of the contract entered into between the Data Subject and Controller;
- if the Automated Processing is necessary according to other legislation in force in the State;
- if the Data Subject has given his / her prior Consent on the Automated Processing.

TRANSFER

Data transfers out of the UAE may be subject to different laws.

The PDPL imposes limitations on the international transfer of Personal Data to outside of the UAE. Similar to the concept of the “adequate jurisdictions” in the EU, the Data Office is expected to approve certain territories as having sufficient provisions, measures, controls, requirements and rules for protecting privacy and confidentiality of personal data. There are also various other exceptions which exporters can rely on, although further details are awaited from the Data Office.

Article 10 of the SVF Regulation requires that customer data (including customer identification and transaction records) are required to be stored and maintained in the UAE.

Article 13 of the ICT in Health Fields Law requires that Health Information and data related to the health services provided in the UAE may not be stored, processed, generated or transferred outside the UAE, unless in the cases defined by virtue of a decision issued by the Health Authority of the relevant emirate in coordination with the Federal Ministry of Health. Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the State, outlines the circumstances in which such Health Information may be transferred outside of the UAE. The Federal level also requirements need to be considered against various Emirate level policies, procedures and guidance documents which, depending upon the location of the relevant parties, patients and the nature of the activities being performed may also impact the collection, processing and international transfer of health information.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the telecommunications services ordered by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information, and use such information only as needed for the provision of the requested services. Telecommunications service providers are required to ensure that the contracts between them and any affiliate or third party holds the other party responsible for the privacy and protection of the subscriber’s information (TDRA Consumer Protection Regulations v1.5, Article 20.8).

SECURITY

The PDPL imposes strict requirements around data security. Controllers and Processors are required to put in place sufficient technical and authorised measures to protect and secure Personal Data, preserve its confidentiality and privacy, and ensuring that such personal data is not breached, destroyed or altered. The measures which must be taken need to take into account the nature, scope and purposes of processing and the possibility of risks to the confidentiality and privacy of the Data Subject’ s Personal Data. Put simply, this means the higher the risk of harm to the Data Subject and / or the higher the likelihood of a breach, the greater the steps to secure personal data that need to be taken.

The UAE's Federal Cabinet has issued Resolution No. 21 of 2013, concerning the Regulation of Information Security in Federal Authorities. Although it applies to information security within UAE federal government bodies, the requirements of this resolution might be passed on to contractors providing services to Federal government bodies when they are entering into service supply agreements with such bodies. Similarly, contractors to emirate level government bodies may need to require with emirate government security standards. Examples, include the Information Security Regulations of the Dubai Electronic Security Center.

Article 20.1 of the TDRA Consumer Protection Regulations v1.5 requires telecommunications service providers to *“take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information”.* Article 20.3 further stipulates that telecommunications service providers must take *“all reasonable measures to protect the privacy of Subscriber Information that it maintains in its files, whether electronic or paper for”*, and that *“reliable security measures”* should be employed.

The UAE Cyber Crime Law focuses on offences related to accessing data without permission and/or illegally (Articles 2 and 3), including financial information (e.g. credit card information or bank account information) (Articles 12 and 13).

Based on the above, best practice from a UAE law perspective 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 adequate enough to minimise the risk of liability arising out of a claim for breach of privacy made by a Data Subject.

BREACH NOTIFICATION

Article 9 of the PDPL requires that the Controller shall, immediately upon becoming aware of any infringement or breach of the Personal Data of the Data Subject that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the Office within such period and in accordance with such procedures and conditions as set by the Executive Regulations. At the date of writing this update, the Executive Regulations have not yet been published.

ENFORCEMENT

The PDPL does not specify penalties, but notes that the Cabinet shall, based on the proposal of the Office General Manager, issue a decision specifying the acts that constitute a violation of the provisions of this Decree Law and the Executive Regulations thereof and the administrative penalties to be imposed.

Despite this there remain possible methods of enforcement of other UAE privacy laws:

1. Where the unauthorised disclosure of personal data results in a breach of the Penal Code

The Public Prosecutor in the Emirate where:

- the party suspected of the breach (‘Offender’) resides; or
- the disclosure occurred,

will have jurisdiction over a Data Subject’s complaint.

If after concluding investigations with the police, the Public Prosecutor is satisfied with the evidence compiled, charges may be brought against the suspect.

The case would then be transferred to the Criminal Courts of First Instance. The Data Subject may attach a civil claim to the criminal proceedings before the Courts have ruled on the case.

Pursuant to Article 432 of the Criminal Law, if the Courts find a suspect who by virtue of his profession, occupation, status, or specialisation has access to a secret but discloses such secret in other than the cases permitted by Law, or who uses such secret for his own benefit or the benefit of another person, unless such disclosure or use is authorised by the concerned person, may be penalized by a fine of at least UAE Dirhams 20,000 (the fine is determined by the Courts) and / or an imprisonment for at least one year.

Similarly, pursuant to Article 431 of the Criminal Law a punishment of *“a jail sentence and a fine”* shall be inflicted on any person who interferes with the right to privacy and family life of individual by:

- eavesdropping, or recording, or transmitting, through a device of any type, conversations done privately or by phone or any other device.
- taking or transmitting, through a device of any type, pictures of any person in private,

unless legally permitted or with the individual’s consent.

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the Data Subject to the Civil Courts of First Instance for further consideration. The Data Subject would need to prove the losses he / she has suffered as a direct result of the disclosure of his / her personal data before the Civil Courts in order for damages to be awarded.

2. Where the unauthorised disclosure of personal data results in a breach of the Cyber Crime Law

The police in each Emirate have developed specialised cybercrime units to handle complaints that relate to breaches of the Cyber Crime Law.

As above, 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 or not 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. The same procedure identified above is then followed before the Courts.

If found guilty of an offence under the Cyber Crime Law, the punishment an Offender can receive varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and / or a fine between AED 150,000 and 5,000,000 (Articles 2, 3, 4, 6, 7, 8 and 45 of the Cyber Crime Law). Notably, Article 13 of the Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes provides that *“Everyone employs information technology or an information technology method to* ***collect, keep or process personal data and information of the nationals or the residents in the state in violation of the legislations in force in the state*** *shall be sentenced to detention and/or to pay fine of not less than (50,000) fifty thousand Dirhams and not more than (500,000) five hundred thousand Dirhams.”* As such, it is likely that this penalty may apply for breaches of the PDPL. 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 57).

3. Where the unauthorised disclosure or transfer of personal data results in a breach of the Central Bank’s Consumer Protection Regulation, Retail Services Regulation or SVF Regulation

The Central Bank may issue administrative and / or financial penalties against Licensed Financial Institutions, SVF Licensees and Payment Service Providers at their discretion. In the case of the Consumer Protection Regulation they may include fines, replacing or restricting the powers of Senior Management or Members of the Board.

4. Where the unauthorised disclosure of personal data results in a breach of the UAE Telecommunications Law and Policies

The TDRA is responsible for overseeing the enforcement of the UAE Telecommunications Law and in this regard may rely on the Police and Public Prosecutor in the Emirate where, either:

- the breach has occurred; or
- where the suspect resides.

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, though a direct approach to the TDRA may be accepted by the them at their discretion (Article 15.11.1 of the TDRA Consumer Protection Regulations v1.5).

The subscriber's complaint needs to be submitted to the TDRA within three months of the date when the service provider last took action . This three months requirement may be waived subject to the discretion of the TDRA (Article 15.11.1 of the TDRA Consumer Protection Regulations v1.5).

After examining the complaint the TDRA may direct the service provider 'to undertake any remedy deemed reasonable and appropriate' (Article 15.11.5 of the TDRA Consumer Protection Regulations v1.5).

ELECTRONIC MARKETING

There are no general laws in the UAE law covering electronic marketing, however the TDRA has issued a regulation governing telecommunications licensees' electronic communications with subscribers, as well as how they should monitor spam passing through their networks. Article 6 of the Cyber Crime Law and Article 20.5 of the TDRA's Consumer Protection Regulation v1.5 are also worded widely enough to potentially apply to electronic marketing.

The TDRA's Unsolicited Electronic Communications Regulation states that telecommunications licensees are under a general obligation to put all practical measures in place to minimise the transmission of Spam having a UAE Link across their Telecommunications Networks, and where they are aware of Spam having a UAE Link sent to or from a particular Electronic Address, they must take all practical means to end the transmission of that Spam and to prevent the future transmission of such Spam. Spam is defined as Marketing Electronic Communications sent to a Recipient without obtaining the Recipient's Consent. Although the Unsolicited Electronic Communications Regulation is targeted and enforced against telecommunications licensees, it effectively puts an obligation upon the licensees to minimise and prevent Spam from being transmitted through their networks.

Federal Decree Law No 14 of 2023 On Trading by Modern Technological Means (“**TMTM Law**”) places further obligations on merchants who trade by modern technological means to protect consumer rights when conducting business.

Article 5 of the TMTM Law places the obligation on merchants to meet the conditions and requirements approved by the competent authorities regarding the advertising and marketing campaigns and the exchange of consumer data.

Article 6 of the TMTM Law provides consumers with the right to choose whether to receive advertising and marketing campaigns or not via phone calls, emails or social media platforms.

ONLINE PRIVACY

The PDPL does not expressly cover online privacy, however the PDPL will apply to Processing online.

Although the UAE Criminal Law does not contain provisions directly relating to the internet, its provisions related to privacy are broadly drafted and therefore could apply to online matters (such as Article 432 as described above).

Additionally, as described in Collection and Processing, under certain circumstances, online privacy is protected through Articles 2, 3, 4, 6, 7, 8 and 44 of the Cyber Crime Law and the TDRA's Consumer Protection Regulation. Unlawful access via the internet, by electronic devices, of financial information (e.g. Credit Cards and Bank Accounts) without permission is a specific offence under the Cyber Crime Law (Articles 6 and 8).

The TMTM Law further provides control on the protection of consumer’s Data and Information within Article 10 of the law. Article 10(1) of the TMTM Law confirms that data protection law in the UAE shall apply to consumer information and data, its classification and ownership.

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.