DIFC

OVERVIEW OF DIFC DATA PROTECTION LAW AND REGULATIONS

Commissioner of Data Protection

CONTENTS

Part 1: Executive Summary

About DIFC

Dubai International Financial Centre (**DIFC**) is a leading international financial hub operating in the Middle East, Africa and South Asia region. It is home to a vibrant business ecosystem of over 25,000 professionals working across more than 2,500 active registered firms that benefit from the centre's robust independent judicial system and regulatory framework that have been designed to align with international standards and best practice.

DIFC operates as an economic free zone and independent jurisdiction within the United Arab Emirates (**UAE**) pursuant to constitutional authority and federal legislation that grants the DIFC's regulatory authorities the power to regulate civil and commercial matters. The DIFC has taken many principles of English common law and codified these principles in the form of specific regulations. In dealing with cases governed by DIFC law, the DIFC Courts may have reference to English Court judgments where English law and DIFC law are consistent. There is also a "waterfall" application of laws that ultimately leads to the application of the principles of English/common law if there is a gap in any relevant DIFC statute.

Data protection in DIFC

In May 2020, pursuant to the powers noted above, the Dubai International Financial Centre (DIFC) Data Protection Law No. 5 of 2020 was enacted by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE, in his capacity as the Ruler of Dubai.

The DIFC Data Protection Law strengthened DIFC's regional leadership in enhancing data protection practices. The original DIFC Data Protection Law enacted in 2004 was the first data privacy legislation in the Arabian Gulf region and it was subsequently updated in 2007 to align more closely to the principles of the EU Data Protection Directive 95/46/EC. The 2020 law and its accompanying regulations sought to combine best practices from a variety of current, world class data protection laws, such as the EU General Data Protection Regulation (**GDPR**), and other forward-thinking legislation such as the California Consumer Privacy Act (**CCPA**). It expanded on the expectations placed on Controllers and Processors in DIFC regarding several key privacy and security principles, as well as introducing innovative measures to support the use of emerging technologies and to implement a more structured approach to responding to government data requests.

These new requirements reflect the DIFC's commitment to developing an enabling business ecosystem with robust regulatory and compliance guidelines for all organisations operating from the Centre. They are intended to enable DIFC to continue to build upon its reputation as a leading global financial centre focused on innovation and collaboration, whilst also promoting ethical data sharing. Importantly, the DIFC Data Protection Law and Regulations were specifically developed with a view to providing a framework that would support DIFC's bid for adequacy recognition by other

jurisdictions, including for example, the United Kingdom, the European Commission and others, easing data transfer compliance requirements for DIFC businesses.

On the launch of the updated DIFC Data Protection Law, His Excellency Essa Kazim, Governor of DIFC commented:

> "*DIFC continues to develop its robust regulatory ecosystem built on the principles of compliance, integrity and security. The enhanced Data Protection Law combines the best practices from world-class data protection laws. By setting out the regulation, DIFC also sets a clear requirement for all organisations to follow global best practice relating to data and privacy. It demonstrates our position as a forward thinking international financial hub shaping the future of finance across the region and enables us to further consolidate the Centre's reputation as a leading global financial centre.*"

The UAE free zone story

DIFC plays a critical role in the financial and commercial ecosystem of the UAE, in particular the Emirate of Dubai. Historically a regional trading hub for ships bringing goods from India and Africa, Dubai created Jebel Ali Port as its first customs-free zone for re-exports in 1980. Five years later, the Jebel Ali Free Zone Authority was established as an independent authority to manage the "jurisdiction". JAFZ became independent of Dubai municipal laws in 1986 and first allowed for the incorporation of single-shareholder free zone establishments (FZEs) in 1992. Sharjah and Dubai subsequently established airport free zones in the mid-90s to facilitate air freight trading. The UAE's Commercial Companies Law was amended in 1998 to carve out the free zones and allow for the establishment of companies in them. JAFZ grew from 19 companies in 1985 to more than 500 by 1995 and is today home to more than 8,000 companies including nearly 100 Global Fortune 500 enterprises.[1]

From 2000 onwards, the number of free zones expanded rapidly, and their focus moved beyond trading and logistics to encompass a range of business sectors including technology, media, education, commodities and healthcare. Key benefits of these zones included proximity to similar businesses, as well as 100% foreign ownership and capital repatriation, flexible setup solutions, and guaranteed "tax holidays" that ensured a 0% corporate and personal income tax rate for (renewable) periods ranging from 15 to 50 years. Certain zones also offered exemptions from customs duties and VAT to facilitate trade.

In 2004, Federal Law No. 8 of 2004 on Financial Free Zones (the Financial Free Zone Law)[2] was passed in the UAE to complement and accelerate the growth of the country's banking and finance sector. The law allowed for the creation of specialist free zones for financial services. Each such zone would have separate juristic and corporate personality with exclusive responsibility for the conduct of its activities. The financial free zones would be expressly exempted from federal civil and commercial

[1] Source: https://jafza.ae/about-us/

[2] Federal Law No. 8 of 2004 on Financial Free Zones

laws with the relevant regulatory authorities given jurisdiction to legislate on most non-criminal matters.

The DIFC was created within this framework pursuant to Federal Decree No. 35 of 2004 and Dubai Law No. 9 of 2004 (as repealed and substituted by Dubai Law No. 5 of 2021[3]). It has developed rapidly to become one of the region's premier destinations for business and financial services by providing global standards to attract leading international financial institutions.

Further details on free zones are available in Section 1.5 below.

DIFC today

As of February 2024, DIFC is home to over 750 regulated firms including top global banks, asset managers and insurance firms. DIFC is also a regional fintech and innovation hub with more than 900 registered fintech and innovation entities providing services including payments, wealth management, digital lending, data analytics and eKYC/AML.[4]

The Centre offers international standards of justice via an English common law framework supported by an independent court system. DIFC's regulatory frameworks are modelled on internationally accepted standards, including in relation to data protection where it has consistently evolved legislation to meet changes in business and legislative practice.

DIFC plays a key and ongoing role in the Emirate of Dubai, which is one of the world's most forward-thinking cities. Among many initiatives to improve the quality of life and make Dubai a city of the future, HH Sheikh Mohammed recently approved the restructuring of the Emirate's Chamber of Commerce into three separate entities including a specialist Chamber of Digital Economy[5] and Smart Dubai[6] – the entity responsible for making Dubai a smart city – has established an AI Ethics Advisory Board to bring together government and private sector entities to explore ethical AI policies, guidelines and tools. The UAE was the first country in the world to appoint a Minister of Artificial Intelligence[7] and DIFC's management is fully aligned with this vision of a responsible and technologically enabled society.

In January 2020, HH Sheikh Mohammed announced the creation of the new Dubai Future District with DIFC at the heart of the new project. DIFC subsequently announced the creation of an Innovation Hub within the District that is intended to play a key role in driving collaboration to accelerate success. DIFC President, His Highness Sheikh Maktoum bin Mohammed bin Rashid Al Maktoum, Deputy Ruler of Dubai,

[3] Dubai Law No 5 of 2021 Concerning the Dubai International Financial Centre
[4] DIFC marks 20th anniversary with record-breaking 2023 performance, exceptional contribution to Dubai's economy. Emirates News Agency – WAM, February 15, 2024.
[5] The National article on restructuring
[6] https://www.smartdubai.ae/
[7] https://www.businessinsider.com/world-first-ai-minister-uae-2017-12

outlined the importance of the DIFC Innovation Hub to the country's aspirations at the launch of the Hub:

> "*The establishment of the DIFC Innovation Hub is an integral part of the strategic roadmap for realising His Highness Sheikh Mohammed bin Rashid Al Maktoum's vision for innovation-driven growth in Dubai. The new facility is a key initiative aimed at generating new economic value by fostering the development of innovation, enterprise and talent across sectors, especially in future-oriented industries. This initiative supports Dubai's aspiration to become a leading global player in shaping the future of vital sectors and creating a thriving international innovation hub in Dubai.*"

In May 2021, HH Sheikh Mohammed issued an update to the DIFC's original founding laws to expand the strategic objectives for DIFC with a view to further boosting Dubai's position as a global hub for financial services and promote the values of efficiency, transparency and integrity. These objectives now also include advancing sustainable economic growth for Dubai, developing and diversifying its economy and increasing the GDP contribution of the financial services sector, to promote investment into Dubai and to attract regional and international entities to establish themselves in DIFC as their principal place of business.

As it continues its growth trajectory in line with those objectives, DIFC is continuing to develop connections to accelerate the future of finance and fintech by fostering collaboration with countries around the world that share a similar vision of a connected global economy.

Part 2: Detailed Analysis of UAE and DIFC Laws and Policies

1 Interplay between DIFC / Federal / Emirate authorities, agencies and laws

1.1 Federal level

1.1.1 The Eastern part of the Arabian Peninsula comprised a collection of tribal sheikhdoms that were subject to various fluctuating foreign influences until the Perpetual Maritime Truce signed between the local rulers and the United Kingdom in 1853. The countries in the Arabian Gulf region that came under the UK's protection as a result of that arrangement became known as the Trucial States. In 1968, the UK government announced that it would be ending all of its treaty and security relationships east of the Suez and, consequently, the United Arab Emirates (**UAE**) was formed as a federation of seven Emirates (Abu Dhabi, Dubai, Sharjah, Fujairah, Ras Al Khaimah, Ajman and Umm Al Quwain) that was declared an independent state on 2 December 1971.

1.1.2 The UAE Constitution[8] was created in 1971 to establish the underlying legal framework by setting out the main rules, rule of law principles, and the political and constitutional organisation of the country.

1.1.3 While the Constitution has many features of other international constitutional documents (including the protection vis a vis rule of law governing certain fundamental rights and freedoms) it is also uniquely tailored to the seven Emirates and reflects many of the political compromises made between them to form the Federation. It explains the main purposes of the establishment of the UAE Federation (amongst others, to protect the rights and liberties of the people of the Federation),[9] identifies the primary Federal authorities[10] and their associated powers and jurisdiction, and establishes the process for promulgating Federal laws[11]. While originally prepared as an interim Constitution intended to last for five years, the Supreme Council eventually adopted it as the country's permanent Constitution in 1996.

1.1.4 The Constitution recognizes that all persons are equal before the law (Article 25), and highlights the UAE's recognition and protection of fundamental rights and freedoms, including inter alia the rights to secrecy and privacy (Article 31 and Article 36);

[8] The UAE Constitution was last amended in 2009.
[9] Article 10, UAE Constitution
[10] The Supreme Council, the President and Deputy President, the Council of Ministers, the Federal National Council and the Judiciary (per Article 45, UAE Constitution)
[11] Articles 110 – 115, UAE Constitution

1.1.5 In addition to the rights and freedoms it sets out explicitly, the Constitution recognizes that "*Foreigners shall enjoy, within the Union, the rights and freedoms stipulated in international charters which are in force or in treaties and agreements to which the Union is party. They shall be subject to the corresponding obligations*." (Article 40).

1.1.6 Accordingly, any access to or processing of Personal Data by public authorities, for example, would have to ensure respect and non-infringement of the above-mentioned fundamental rights and freedoms as set out in the Constitution.

1.1.7 The UAE Constitution grants exclusive legislative and executive jurisdiction to the Federation in respect of the following areas:[12]

a) *foreign affairs (save that individual Emirates may conclude limited agreements of a local and administrative nature with the neighbouring state or regions subject to informing the Supreme Council in advance);*
b) *defence and the UAE Armed Forces;*
c) *protection of the UAE's security against internal or external threat;*
d) *matters pertaining to security, order and jurisdiction in the permanent capital of the UAE;*
e) *matters relating to UAE officials and UAE judges;*
f) *federal finances and federal taxes, duties and fees;*
g) *federal public loans;*
h) *postal, telegraph, telephone and wireless services;*
i) *the construction, maintenance and improvement of UAE roads which the Supreme Council has determined to be trunk roads and the organisation of traffic on such roads;*
j) *air traffic control and the issue of licences to aircraft and pilots;*
k) *education;*
l) *public health and health services;*
m) *currency notes and coins;*
n) *weights, measures and standards;*
o) *electricity services;*
p) *UAE nationality, passports, residence and immigration;*
q) *UAE property and all matters relating thereto;*
r) *census matters and statistics relevant to federal purposes; and*
s) *federal information.*

1.1.8 The Federation is also solely responsible for enacting laws in the following matters:[13]

a) *labour relation and social security;*
b) *real estate ownership and expropriation for public interest;*
c) *extradition of criminals;*

[12] Article 120, UAE Constitution
[13] Article 121, UAE Constitution

d) *banks;*
e) *insurance of all kinds;*
f) *protection of agriculture and animal wealth;*
g) *major legislation related to penal, civil and commercial codes, company law, and civil and criminal procedural codes;*
h) *protection of intellectual, technical and industrial property rights, copyright, printing and publishing rights;*
i) *import of arms and ammunitions unless the same was for the use of the Armed Forces or Security Forces of any Emirate;*
j) *other aviation matters outside the jurisdiction of the Federation;*
k) *delimitation of territorial waters and regulation of navigation in the high seas;*
l) *regulation of financial free zones, the manner in which they are established and how far they are excluded from the scope or application of Federal laws.*

1.2 Emirate level

1.2.1 Each of the seven Emirates have their own government overseen by the relevant ruling family. These local governments vary in complexity depending on the size and development of the relevant Emirate, but most (including Dubai) have their own executive councils and departments reflecting the various federal ministries. The Emirate-level governments function in tandem with the Federal government.

1.2.2 The individual Emirates are obliged to undertake appropriate steps to implement laws promulgated by the Federation and the treaties and international agreements concluded by the Federation. Otherwise, each Emirate has jurisdiction within its own geographic borders in all matters not assigned to the exclusive jurisdiction of the Federation (see paragraph 1.1 above).[14] Additionally, each Emirate is required to respect the independence and sovereignty of the other Emirates in their internal affairs within the framework of the Constitution.[15]

1.2.3 The UAE Constitution is supreme: its provisions prevail over any constitutions of the member Emirates and federal laws have priority over any Emirate-level legislation. If a conflict exists between a Federal and Emirate law, the Emirate legislation which is inconsistent with the Federal legislation "shall be rendered null and void to the extent that it removes the inconsistency" and any dispute between Federal and Emirate laws is handled by the Federal Supreme Court.[16]

[14] Article 122, UAE Constitution
[15] Article 10, UAE Constitution
[16] Article 151, UAE Constitution

1.3 Dubai Government

1.3.1 Dubai is ruled by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the United Arab Emirates and Ruler of Dubai.

1.3.2 The Executive Council is the main legislative government body in the emirate of Dubai and is chaired by His Highness Sheikh Hamdan bin Mohammed bin Rashid, Crown Prince of Dubai. The Executive Council supervises, and guides government policies and services so that they are underpinned by four main pillars: integrated government services; government excellence; strategies, policies and corporate governance; and integrated government communications.

1.3.3 In addition to the Executive Council, there are more than 50 other Dubai government departments.[17]

1.4 UAE judicial system

1.4.1 The UAE has a varied legal system comprising a mixture of civil law, Sharia laws and (in the free zones of DIFC and ADGM) common law. The civil law system is derived from the Egyptian and French civil codes and includes the majority of civil and criminal laws in codified form. The Sharia law system operates in parallel, particularly in relation to family matters in the personal status courts. The Sharia courts have exclusive jurisdiction in relation to family disputes (e.g. divorce, inheritance, child custody and guardianship) and Islamic marriages are conducted in accordance with Sharia provisions. Sharia principles are reflected in the UAE's commercial laws.

1.4.2 The judicial system of the UAE comprises both a federal judiciary (comprising courts of first instance and appeal courts presided over by the Federal Supreme Court, also known as the Court of Cassation) and local judicial departments with each Emirate free to participate in the federal judiciary or maintain its own system. Currently, Abu Dhabi, Dubai and Ras Al Khaimah maintain their own independent judicial departments (applying Federal laws within their respective Emirate) while the remaining Emirates follow the federal system.

1.4.3 The UAE Constitution states that judges must be independent and subordinate to no authority but the law and their own consciences in the performance of their duties.[18]

1.4.4 The UAE Constitution establishes the Federal Supreme Court which is stated to consist of a President and a number of Judges (not exceeding five in total) who are appointed by Decree issued by the President after approval by the

[17] See https://tec.gov.ae/en/web/tec/dubai-government-entities
[18] Article 94, UAE Constitution

Supreme Council (see 0 for details of the process of issuing federal legislation).

1.4.5 The Federal Supreme Court is competent to render judgment in relation to:

(a) *disputes between member Emirates;*

(b) *examination of the constitution legality of Federal laws (if challenged by one or more of the Emirates) and Emirate legislation (if challenged by one of the Federal authorities);*

(c) *examination of the constitutional legality of laws, legislation and regulations generally (pursuant to a request submitted by a State Court, in which case the relevant State Court is bound to accept the Federal Supreme Court's ruling);*

(d) *interpretation of the provisions of the Constitution, when requested by any Federal authority or by the Government of any Emirate;*

(e) *interrogation of Ministers and senior Federal officials concerning their actions in the conduct of their official duties;*

(f) *crimes directly affecting the interests of the Federation (e.g. crimes relating to national security);*

(g) *conflicts of jurisdiction between Federal and Emirate judicial authorities;*

(h) *conflicts of jurisdiction between judicial authorities in different Emirates; and*

(i) *any other jurisdiction stated in the Constitution or assigned by Federal law.*

1.4.6 The judgments of the Federal Supreme Court are stated to be finding and binding upon all.[19]

1.4.7 Federal Courts of First Instance have jurisdiction to hear:

(a) *civil, commercial and administrative disputes between the UAE and individuals;*

(b) *crimes committed within the UAE, unless reserved to the Federal Supreme Court;*

(c) *personal status actions, civil actions, commercial actions and other actions between individuals in the UAE.*

1.4.8 Below the Federal courts, the local judicial authorities in each Emirate have jurisdiction in all judicial matters not assigned to the Federal judiciary.

[19] Article 101, UAE Constitution

1.4.9 The common law DIFC courts have been in operation since 2007. Both are English language, common law judiciaries with jurisdiction to hear civil and commercial disputes. In particular, as per the 2009 Protocol of Jurisdiction between DIFC Courts and Dubai Courts,[20] the DIFC Courts have exclusive jurisdiction over:

(a) *civil or commercial cases and disputes involving the Centre or any of the Centre's Bodies or any of the Centre's companies, and branches of companies and establishments that are established or licensed to operate in the DIFC;*

(b) *civil or commercial cases and disputes arising from or related to a contract that is to be or has been performed in whole or in part within the DIFC.*

(c) *civil or commercial cases and disputes arising from or related to a transaction that has taken place, in whole or in part, in the Centre, and which is related to Financial Banking Activities, Financial Activities, Ancillary Activities or any Activities licensed to be performed within the DIFC;*

(d) *civil or commercial cases and disputes arising from or related to an incident that has occurred in the Centre, except Criminal Proceedings relating to any Criminal Offence according to the Penal Codes; and*

(e) *disputes about Civil remedies flowing from or related to any criminal Offence that has occurred in the Centre.*

1.4.10 The jurisdiction of the individual courts within the DIFC Courts is set out in Article 5 of Dubai Law No. 12 of 2004 (Judicial Authority Law)[21] and the application of laws in the DIFC Courts is established by DIFC Law No. 3 of 2004 (Law on the Application of Civil and Commercial Laws in the DIFC).[22] See also paragraph 0 below for further detail on the application of laws in DIFC.

1.4.11 The DIFC Court is considered part of the Dubai court system and has been used as a conduit to enforce foreign judgments in the UAE based on:

(a) *a general jurisdiction to enforce foreign court judgments under Article 7(6) of the Judicial Authority Law and Article 24(1)(a) of DIFC Law No. 10 of 2004 (the **DIFC Court Law**);[23] and*

(b) *the principle set out in Article 7(2) of the Judicial Authority Law which states that judgments, decisions and orders rendered by the DIFC Courts shall be executed by the onshore courts.*

---

20 https://www.difccourts.ae/about/protocols-memoranda/protocol-jurisdiction-between-difc-courts-and-dubai-courts

21 https://www.difc.ae/files/7014/5510/4276/Dubai_Law_No._12_of_2004_as_amended_English.pdf

22 Law on Application of Civil and Commercial Laws in DIFC

23 https://www.difc.ae/application/files/7015/9602/1158/Court_Law_DIFC_Law_No.10_of_2004.pdf

While the conduit nature of the DIFC Courts has been challenged, recent decisions of the Joint Judicial Committee that was established to deal with conflicts of jurisdiction between the Dubai Courts and the DIFC Courts have allowed claims to continue in DIFC Courts despite attempts to use the Committee to block enforcement actions.[24]

1.4.12 The DIFC Courts have also entered into a memorandum of guidance as to reciprocal enforcement with the English Commercial Court.[25]

1.4.13 There is no formal system of binding precedent in the UAE. However, in practice, certain precedents are followed and some judgments of higher courts are published. The DIFC courts are common law courts and do adopt a system of binding judicial precedent, as well as frequently referring to English and other common law judgments.

1.5 Free zones

1.5.1 Under the 2004 Constitutional Amendment, the UAE Federation has the legislative power to regulate the financial free zones, determine how they are established and how far they are excluded from the scope of application of Federal laws.[26]

1.5.2 As the UAE has transformed from a subsistence economy to one of the most prosperous and highly advanced societies in the world, the government has adopted a policy of controlled diversification to move the economy away from reliance on oil. The concept of the free trade zones was to create specific geographic areas with special laws aimed at encouraging new business and attracting this foreign investment.

1.5.3 There are now numerous free trade zones established in the UAE, which operate as semi-autonomous jurisdictions with separate tax, customs and imports regimes and (in some cases) governed by their own legal frameworks and court systems. These zones will typically be set up to attract particular types of business or business activity, the first such zone being established around the Jebel Ali port for trading businesses and subsequent zones now dedicated to sectors including technology, design, media, commodities and healthcare.

1.5.4 Financial free zones are established by federal legislation as free zones for financial services activities and their powers are prescribed by the Federal Cabinet. Federal Law No. 8 of 2004 (**Financial Free Zone Law**) states that:

[24] https://www.clydeco.com/en/insights/2020/02/joint-judicial-committee-takes-a-stand-against-blo
[25] https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Guidance/uk-uae-protocol-with-logos.pdf
[26] Article 121, UAE Constitution

> "*The financial free zone shall be established by virtue of a federal decree. It shall have a juridical personality and shall be duly represented by the Chairman of the Board of Directors thereof. It shall be solely liable for the commitments resulting from the practice thereby of the activities thereof. The Cabinet shall specify the location and area thereof*".[27]

Moreover, financial free zones are defined as an independent jurisdiction within the UAE with the power to establish their own regulatory frameworks.

1.5.5 The Financial Free Zone Law exempts financial free zones and the financial activities within such zones from all Federal civil and commercial laws: "All financial zones and activities shall be subject as well to the provisions of the Federal Laws, with the exception of the civil and commercial federal laws".[28] Financial free zones, therefore, have the power to regulate civil and commercial matters.

1.5.6 The Financial Free Zone Law also confirms the application of Federal criminal laws in the financial free zones, which would include Federal legislation on anti-money laundering, the Cybercrimes Law and the Penal Code (as defined and described in paragraph 3.1 below).

1.5.7 Cabinet Resolution No. 28/2007 on the Implementing Regulation of Federal Law No 8/2004 on the Financial Free Zones states that any company or institution that wishes to practice the activities of the free zone "outside the borders of the financial free zones yet within [the UAE] shall be subject to the federal laws in force in [the UAE], including the civil and commercial federal laws, the implementing decisions thereof and the procedures adopted in this regard."[29]

1.5.8 Companies that operate outside the financial free zones, therefore, will need to comply with the federal laws of the UAE, while those that conduct business within the financial free zones are subject to the laws of the respective zone.

1.5.9 DIFC is a Financial Free Zone.

[27] Article 2, Financial Free Zone Law
[28] Article 3, Financial Free Zone Law
[29] Article 3(3), Financial Free Zone Law

2 Authority of the DIFC

2.1 Powers derived from UAE Federal Authority

2.1.1 Dubai International Financial Centre (DIFC) was established as the first financial free zone in the UAE shortly after the enactment of the Financial Free Zone Law. Accordingly, the DIFC operates pursuant to:

(a) *the Federation's exclusive jurisdiction over banks and insurance activities in the UAE as provided for under the Constitution and, in particular, the 2004 Constitution Amendment;*

(b) *the Financial Free Zone Law (as the Federal legislation issued pursuant to Article 121 of the amended UAE Constitution to regulate financial free zones); and*

(c) *Federal Decree No. 35 of 2004 (the **DIFC Law**), which establishes "a* financial free zone named 'Dubai International Financial Center*"*[30] *pursuant to the Financial Free Zone Law and its Implementing Regulation.*

2.1.2 Accordingly, the DIFC has the power to issue legislation necessary for the DIFC and those bodies and establishments operating within the DIFC. Since Federal civil and commercial laws do not apply within the DIFC (as per the Financial Free Zone Law), the DIFC is empowered to create its own legal and regulatory framework for all civil and commercial matters.

2.2 Powers derived from Dubai Emirate Authority

2.2.1 The Implementing Regulation to the Financial Free Zone Law provides each Emirate with the right to issue necessary legislation for the establishment of a financial free zone. Dubai Law No. 9 of 2004 concerning the Dubai International Financial Centre was superseded by Dubai Law No. 5 of 2021 concerning the Dubai International Financial Centre (**the DIFC Dubai Law)**[31] to establish the objectives and set up the core DIFC bodies. It applies to:

(a) *the DIFC "*as a financial free zone having financial and administrative autonomy, and affiliated to the Government"*;*[32]

(b) *the DIFC Bodies established under Dubai Law 5 of 2021, including:*

(i) the Dubai International Financial Centre Authority (**DIFCA**);

[30] Article 1, DIFC Law
[31] Law No. 5 of 2021 Concerning DIFC
[32] Article 3(a)(1), DIFC Dubai Law

(ii) the Dubai Financial Services Authority (**DFSA**);

(iii) the Dubai International Financial Centre Courts (**DIFC Courts**); and

(iv) any boards, bodies, offices, committees, registries, corporations, departments, or entities which are established under Dubai Law No. 5 of 2021, the DIFC Laws, or the DIFC Regulations; or which are established pursuant to the provisions of the DIFC Dubai Law; and

(c) *the geographical area delimited in Federal Law No. 8 of 2004 as the site of the DIFC.*

2.2.2 The DIFC Dubai Law sets out the powers of the DIFC authorities, including the right of the DIFCA Board of Directors to "*propose draft DIFC Laws… and submit the same to the President for approval, in preparation for final approval and issuance by the Ruler*".[33]

2.2.3 The DIFC Dubai Law exempts the DIFC, DIFC Bodies (as noted above) and DIFC Establishments (i.e. entities or businesses established, licensed, registered or authorised to operate or to conduct activity within or through the DIFC) from Emirate-level laws and regulations in Dubai as follows:

> "*Except for legislation relating to the environment, health, public safety, and food control in force in the Emirate, the DIFC, DIFC Bodies, DIFC Establishments, the staff and employees of any of them or the Persons authorised by them, and the land, real estate, and property located in the DIFC, will not be governed by the legislation issued by the Government* [of Dubai] *or by any local Government Entity in the Emirate, except as may be provided for by a special provision in such legislation*."[34]

2.2.4 DIFCA is provided with legal personality and financial, administrative and operational independence as necessary to enable it to enter into legal acts and perform its functions.[35]

2.2.5 As per the Implementing Regulation to the Financial Free Zone Law, the DIFC is provided with powers to regulate areas in the DIFC that are not specifically prescribed to the Emirate of Dubai (i.e. matters relating to the environment, food control, public health and safety as noted in the extract from the DIFC Dubai Law at paragraph 2.2.3 above).

2.2.6 The DIFC has taken many principles of English common law and codified these principles in the form of DIFC legislation. In dealing with cases governed by DIFC law, the DIFC Courts may have reference to English Court

[33] Article 9(b)(3), DIFC Dubai Law
[34] Article 22(b), DIFC Dubai Law
[35] Article 8(a), DIFC Dubai Law

judgments where English law and DIFC law are consistent. This application of laws is codified in the Law on the Application of Civil and Commercial Laws in the DIFC, which outlines a "waterfall" of applicable laws beginning with DIFC law and ultimately concluding with the law of England and Wales.[36] This interpretation has been followed in DIFC case law.[37]

2.3 Data protection in the DIFC

2.3.1 In light of:

(a) *the exemption of application of Federal civil and commercial laws under the Financial Free Zone Law (see paragraph 1.5.5 above);*

(b) *the designation of DIFC as a Financial Free Zone pursuant to the Financial Free Zone Law by way of the DIFC Law (see paragraph 2.1.1 above);*

(c) *the establishment of the DIFC Bodies and incorporation of the DIFC as a financial free zone in Dubai with administrative autonomy pursuant to the DIFC Dubai Law (see paragraph 2.2.1 above);*

(d) *the powers granted to the DIFCA Board of Directors to issue laws applicable within the jurisdiction of the DIFC in areas other than those expressly reserved (see paragraphs 2.2.2 to 0 above),*

the DIFC first enacted a Data Protection Law on 16 September 2004 (DIFC Law No.9 of 2004).[38] The 2004 legislation was subsequently amended by the DIFC Laws Amendment Law 2005, DIFC Law No. 2 of 2005 on 19 April 2005.

2.3.2 The Data Protection Law 2007 (DIFC Law No.1 of 2007)[39] replaced the 2004 law and abrogated the Data Protection Module issued by the DFSA, which was replaced by the Data Protection Regulations 2007. The 2007 legislation was subsequently amended by Data Protection Law Amendment Law, DIFC Law No.5 of 2012 and by DIFC Laws Amendment Law, DIFC Law No. 1 of 2018.

[36] Article 8(2), Law on the Application of Civil and Commercial Laws in the DIFC

[37] See, for example, paragraph 17 of the judgment in Lural v (1) Listran (2) Lokhan [2021] DIFC CA 003 (https://www.difccourts.ae/rules-decisions/judgments-orders/court-appeal/lural-v-1-listran-2-lokhan-2021-difc-ca-003)

[38] https://dfsaen.thomsonreuters.com/sites/default/files/net_file_store/DFSA_7603_VER2.pdf#:~:text=DATA%20PROTECTION%20LAW%20DIFC%20Law%20No.9%20of%202004,Law%20No.2%20of%202005%20on%2019%20April%202005

[39] https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

2.3.3 The current law, the Data Protection Law, DIFC Law No. 5 of 2020 (the "DPL" or "DIFC DPL") [40] was enacted on 21 May 2020. It repealed the 2007 legislation and came into effect on 1 July 2020. The DIFC DPL is supplemented by the Data Protection Regulations that came into force on the same date.[41] The DPL was amended and an updated version published in March 2022.[42]

2.3.4 Each of the above-referenced laws was enacted pursuant to an Enactment Notice signed by the Ruler of Dubai.

2.3.5 The exclusive authority of DIFCA to regulate on the area of data protection is reinforced by the consultative process, whereby Federal and Emirate level government authorities provide drafts of legislation on data protection and information security so that DIFCA can provide commentary. The drafting of UAE or Dubai legislation normally excludes applicability in the financial free zones, or at least provides DIFCA the opportunity to oppose any application. The most recent example is the draft national data protection legislation that expressly excludes applicability in the financial free zones, which DIFCA supported in its consultative feedback. DIFCA further suggested an adequacy mechanism so that DIFCA and any relevant jurisdiction subject to the draft law could engage in a formal assessment and decision-making process.

2.4 DIFC Commissioner of Data Protection

2.4.1 The DIFC DPL grants the President of the DIFC the power to appoint a person to administer the Law (the Commissioner).[43] The Commissioner is appointed for a specified term of up to five years and the President is required to consult with the DIFCA Board of Directors prior to the appointment, re-appointment or removal of the Commissioner.

2.4.2 The Commissioner's powers, duties and functions are set out in Part 8 of the DIFC DPL. The Commissioner's statutory objectives in performing his functions and exercising his powers are:

(a) *to monitor, ensure and enforce compliance with the DIFC DPL;*

(b) *to promote good practices and observance of the requirements of the DIFC DPL and the Regulations by Controllers and Processors; and*

[40] https://www.difc.ae/business/laws-regulations/legal-database/data-protection-law-difc-law-no-5-2020/
[41] DIFC DPL 2020
[42] DIFC DP Regulations
[43] Article 43(1), DIFC DPL

(c) *to promote greater awareness and public understanding of data protection and the requirements of the DIFC DPL and the Regulations in the DIFC.*[44]

2.4.3 The Commissioner has powers to audit Controllers and Processors, to conduct investigations and inspections to verify compliance, to issue directions, initiate proceedings and impose fines for non-compliance, as well as preparing draft regulations, standards/codes of practice or guidance for approval of the DIFCA Board of Directors.[45]

2.4.4 In addition to monitoring and enforcing compliance with the DIFC DPL, DIFCA and other DIFC bodies and offices (including the Commissioner) contribute to the wider governmental structure in the UAE. In this context, the DIFC is asked to contribute from time to time on various developments and the Commissioner's Office has been involved since 2019 with discussions around the development of a national data privacy law and supervisory authority's office. Representatives of the Commissioner's Office have attended meetings and provided feedback during the internal government consultation process, it being recognised that any new national legislation in this area could benefit from the experience of the existing regulatory regimes in the financial free zones such as DIFC and from aligning with those existing systems.

3 UAE legislative protection for Personal Data (ex-DIFC)

3.1 National/federal laws of general application

3.1.1 The UAE enacted a standalone data protection law as a framework that will regulate the collection, storage, processing and transfer of Personal Data in the UAE. It is based on the European GDPR-style principles and obligations. In addition, GDPR-style concepts can be seen in provisions of more recent Federal legislation such as the Healthcare ICT Law and the IoT Policy (see further below).

3.1.2 While the UAE has not directly entered into any international commitments in the data protection space, Federal government ministers have been quoted on the importance of strong data protection legislation. Furthermore, the regulators of the two financial free zones have been active in this area, for example in 2020, DIFC became the region's first fully accredited member of Global Privacy Assembly[46] and actively supports the GPA by leading a working group within the Covid-19 Task Force / Data Sharing for the Public Good working group, as well as participating in Policy and Strategy and the International Enforcement working groups. DIFC also became a member of GPEN in early 2021.

[44] Article 46(2), DIFC DPL
[45] Article 46(3), DIFC DPL
[46] https://www.zawya.com/saudi-arabia/en/business/story/DIFC_becomes_member_of_Global_Privacy_Assembly-SNG_186984593/

3.1.3 Notwithstanding the lack of a standalone law, there are a range of legislative provisions under UAE federal laws that protect the privacy of Personal Data and/or regulate the processing of Personal Data. Federal legislation relevant to data protection and processing includes the following laws of general application:

(a) *the UAE Constitution;*
(b) *Federal Law No. 3 of 1987 (the **Penal Code**);*
(c) *Federal Law No. 1 of 2006 concerning e-transactions (**E-Commerce Law**);*
(d) *Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes (**Cybercrime Law**); and*
(e) *Federal Law No.15 of 2020 on Consumer Protection (**Consumer Protection Law**).*

UAE Constitution

3.1.4 The UAE Constitution allows for a general concept of privacy and, in accordance with Article 31 of the Constitution, individuals are entitled to the freedom of communication by post, telegraph or other means of communication and the secrecy of those communications is guaranteed in accordance with the law.

3.1.5 The Constitution also provides every person with the right to submit complaints to the competent authorities, including the judicial authorities, concerning the violation of any of their rights and liberties set forth in Part 3 of the Constitution, which includes Article 31.[47]

Penal Code

3.1.6 The Penal Code criminalises the unauthorised disclosure of "secret" information as it may be considered an invasion of privacy.

3.1.7 Under the Penal Code, it is an offence for an individual who is entrusted with a secret by reason of their profession or situation to disclose that secret in any situation (other than those permitted by law) or to use the secret for their or another person's advantage, unless the individual to whom the secret pertains has consented for it to be disclosed.[48]

3.1.8 Individuals can also be held liable under Article 378 for a fine or a custodial sentence in circumstances in which, through any means of publicity, the individual publishes news, pictures or comments pertaining to the secrets of a person's private or family life, even if such publications are true.

[47] Article 41, UAE Constitution
[48] Article 379, Penal Code

3.1.9 The Penal Code also provides that any person who unlawfully reproduces, distributes or provides others with the contents of a telephone call, message, information, data or other issues which came to his knowledge by virtue of his work shall be punished by a jail sentence.[49]

3.1.10 "Publication" in the context of Article 378 has been widely interpreted by the local courts to cover any disclosure of personal information and, as such, this provision acts to regulate significant amounts of Personal Data processing.

3.1.11 The term "secrets" is not defined under the UAE Constitution nor the Penal Code, so a range of judicial interpretations is possible. It may be possible, for example, that an individual who objects to their data being shared with a third party without their permission could seek to initiate criminal proceedings based on the Penal Code provisions.

E-Commerce Law

3.1.12 Privacy is specifically protected in an electronic context in the E-Commerce Law. The E-Commerce Law provides that any person who has obtained access to electronic information, electronic records, electronic documents, or electronic correspondence and has divulged any such information shall be liable to a minimum of six months' imprisonment and a fine between AED 20,000 (approx. GBP 4,000) and AED 200,000 (approx. GBP 40,000).[50]

Cybercrimes Law

3.1.13 Federal Law No. 12 of 2016 amending Federal Law No. 5 of 2012 on combating cybercrimes (Cybercrimes Law) sets out a range of offences which may be perpetrated on electronic information systems or over information networks. The Cybercrimes Law prohibits the invasion of an individual's privacy using information technology to, amongst other methods, overhear, intercept, record, transfer or disclose conversations or communications unless otherwise authorised by law or with the consent of the individual.[51] Article 15 of the Cybercrimes Law in particular states that it is an offence for persons to intentionally and without permission capture and/or intercept communications online.

3.1.14 Under the Cybercrimes Law and the Penal Code, therefore, if the collection, processing and transfer of any Personal Data pertains to an individual's secret or private or family life, then a lawful reason or consent is required to disclose such data.

3.1.15 Criminal and civil penalties can be imposed for a breach of the Penal Code and the Cybercrimes Law: a fine of at least AED 20,000 (approx. GBP 4,000) and/or imprisonment for at least one year under the Penal Code and a fine

[49] Article 380(bis), Penal Code
[50] Article 28, E-Commerce Law
[51] Articles 21 and 22, Cybercrimes Law

between AED 150,000 (approx. GBP 30,000) and AED 1 million (approx. GBP 200,000) and/or minimum imprisonment of six months under the Cybercrimes Law.

3.1.16 UAE Law No. 35 of 1992, as amended (**Criminal Procedures Law**) permits any person who sustains a loss from a crime to pursue their civil rights before the criminal courts during the criminal proceedings.

Consumer Protection Law

3.1.17 A new Consumer Protection law was issued in late 2020 to govern the sale of all goods and services in the UAE (whether "onshore" or in the free zones) and related activities carried out by suppliers, advertisers and other parties.

3.1.18 The Consumer Protection Law establishes the protection of consumer privacy as a consumer right. It contains a general obligation on businesses that supply consumers to protect consumer data and a prohibition on using such data for marketing purposes. It is anticipated that further detail will be provided in the executive regulations to the law (which have yet to be published as at the date of this memorandum) and whether this provision constitutes a complete ban on the use of Personal Data for marketing and promotional purposes.

3.1.19 There are also requirements for e-commerce providers to provide certain information to consumers and competent authorities, as well as an obligation to ensure that "data, advertising and contracts relating to the consumer" are provided in Arabic. Again, further details are anticipated to be provided in the executive regulations.

3.1.20 Penalties under the new Consumer Protection Law for certain offences could involve fines of up to AED 2 million (approx. GBP 400,000) and imprisonment for up to two years (with these penalties doubled for repeat violations). Other sanctions may include confiscation or destruction of offending items, closure of the establishment and publication of the conviction. The law provides a one-year grace period for affected entities to ensure compliance, which will expire in November 2021.

3.2 Sector-specific regulation

3.2.1 In addition to the federal laws set out above, there are numerous sector-specific laws governing a number of national industries or specific data types:

Healthcare sector

3.2.2 In addition to a core doctor-patient confidentiality requirement that is codified in Federal Law No. 7 of 1975 concerning the practice of human medicine profession (**Medical Profession Law**), the UAE issued Federal Law No. 2 of 2019 on the use of information and communication technology in the areas of

health (**Healthcare ICT Law**) to regulate the use of technology in the UAE healthcare sector. The Healthcare ICT Law applies to all "health data which has been processed and given a visual, audible or readable meaning and which may be attributed to the health sector" (**Health Data**). It therefore regulates the processing of all Health Data regardless of its form, including the names of patients, information collected during consultation, diagnosis, treatment, research and lab results.

3.2.3 The Healthcare ICT Law sets out a number of data protection obligations and restrictions, including:

(a) *keeping Health Data confidential;*
(b) *ensuring Health Data is accurate and reliable;*
(c) *keeping Health Data secure by putting in place measures to protect Health Data and to prevent any unauthorised processing, damage, alteration, deletion or amendments;*
(d) *ensuring that only authorised personnel have access to Health Data; and*
(e) *retaining Heath Data for a minimum period of 25 years from the date on which the last procedure on a patient was conducted, or as long as is necessary, if longer.*

3.2.4 The Healthcare ICT Law has a broad application within the UAE. It is a federal law that applies throughout the UAE, including the free zones such as the DIFC. Where there are inconsistencies between the Healthcare ICT Law and an Emirate level or free zone law, the Healthcare ICT Law will apply to the extent of the inconsistency. However, since the obligations imposed by the Healthcare ICT Law on the use of medical data are stringent, the Healthcare ICT Law provides additional protection on the processing of medical data, supplementing the requirements under the DIFC Data Protection Law. In practice, these obligations are implemented by the local health authorities in the data controls and standards imposed in relation to their platforms (e.g. Dubai Healthcare Authority's NABIDH platform[52] or Abu Dhabi's equivalent Malaffi system)[53] and the Federal Ministry of Health & Prevention has announced an intention to link these with the National Unified Medical Records platform, Riayati.[54]

3.2.5 The Healthcare ICT Law is relevant to all healthcare providers, insurers and entities providing healthcare IT services. It also applies to those entities operating in the UAE which are, directly or indirectly, engaged in activities that involve handling of electronic health data, covering providers of outsourcing services to the health sector such as cloud service providers.

[52] https://nabidh.ae/#/comm/policies
[53] https://malaffi.ae/what-is-malaffi/policies/
[54] https://www.mohap.gov.ae/en/MediaCenter/News/Pages/2725.aspx

3.2.6 Additionally, the Healthcare ICT Law establishes a general rule that any entity that processes patient information must keep the data confidential and not use them for non-medical purposes without the written consent of the patient.[55] The Implementing Regulation provides further information on confidentiality and encryption measures, as well as an obligation to report activities that may affect the confidentiality of health data. Certain exceptions to this rule apply, including when the Health Data is processed for insurance purposes or the use of the patient's information is for scientific and clinical research; provided that, for the latter, the identity of the patient is not disclosed and applicable scientific research standards and guidelines are complied with.[56]

3.2.7 Another key feature of the Healthcare ICT Law is a data localisation requirement that provides for a general prohibition on the transfer, storage, generation or processing outside the UAE of Health Data related to health services provided within the UAE. Health Data therefore must be processed and stored inside the UAE and cannot be transferred outside the UAE unless an exception is issued by the relevant health authority. Certain exceptions are contained in Ministerial Decision No. 51 of 2021 on permitted cases for storing and transferring medial data outside the State (the **Health Data Transfer Regulation**). These exceptions include transfers carried out in the context of lawful scientific research (i.e. complying with UAE laws), insurance claims (where the patient has consented to the overseas transfer) and where individual patient requests the data to be to be transferred outside the UAE or to receive them for use abroad (subject to receiving an "official request" from the individual or their legal representative). The Health Data Transfer Regulation also contains conditions for certain types of transfer, including the use of encryption and the implementation of "the highest safety standards".

3.2.8 A breach of key requirements of the Law, such as the data localisation and confidentiality obligations, may lead to penalties ranging from warnings to fines of AED 1 million (approx. GBP 200,000) and/or cancelling a business' registration or permit to use the centralised healthcare system.

Financial sector

Credit Information Law

3.2.9 Under Federal Law No. 6 of 2010 (Credit Information Law) and Cabinet Resolution No. 16 of 2014 (the CIL Regulations), the Al Etihad Credit Bureau was established to provide a single source of reliable data regarding credit information of natural and legal persons in the UAE. The purpose of the Credit Bureau was to enable lenders to better assess the creditworthiness of prospective borrowers.

3.2.10 The Credit Information Law and the CIL Regulations incorporate several data protection standards as follows:

[55] Article 16, Healthcare ICT Law
[56] Article 16(2), Healthcare ICT Law

(a) *the collection and circulation of data or details that relate to a person's private life, opinions, beliefs or health condition is prohibited;*

(b) *consent of the Data Subject is required before issuing any credit information reports relating to such person;*

(c) *information can only be used for the purposes for which it was provided;*

(d) *recipients of credit information must keep such information confidential;*

(e) *the Credit Bureau is required to use modern systems to maintain credit information and to implement suitable security and information security mechanisms; and*

(f) *Data Subjects should be provided with the right to request the correction of errors relating to his or her credit information.*

3.2.11 The Credit Information Law includes civil and criminal penalties for certain offences. For example, anyone who reveals credit information other than as authorised by the Credit Information Law or the CIS Regulations can be exposed to a fine of AED 50,000 (approximately £10,000) and up to two years' imprisonment. The same penalty applies to anyone who obtains credit information without obtaining the approvals required pursuant to the Credit Information Law or the CIS Regulations, or by using fraudulent methods or incorrect information.

3.2.12 The Central Bank of the UAE (**CBUAE**) issued Regulatory Framework for Stored Values and Electronic Payment Systems (**E-Payment Regulation**) in 2017, which includes a number of restrictions on the way digital payment service providers (**Payment Providers**) store and process users' data.

3.2.13 The E-Payment Regulation requires Payment Providers to have in place adequate data protection policies, measures and procedures to protect customer data from unauthorised access, retrieval, tampering and misuse. Payment Providers are also required to store all customer data (including customer identification and transaction records) in the UAE for a minimum of five years.

Central Bank Consumer Protection Framework

3.2.14 The CBUAE recently established a Financial Consumer Protection Regulatory Framework that introduces requirements for the protection of clients' Personal Data.[57]

[57] The CBUAE issued the Consumer Protection Regulation (CPR) in December 2020 followed by the Consumer Protection Standards in January 2021.

3.2.15 The Framework draws upon a broad range of principles premised on international standards which enhance the competitiveness, integrity and stability of the UAE's banking sector. The protection of consumer's Personal Data and privacy is one of the many protections offered by the Framework.

3.2.16 The Framework applies to all licensed financial institutions (**LFIs**) whether incorporated in the UAE or in other jurisdictions, or having a branch, subsidiary or representative office in the UAE that are licensed by the CBUAE to carry out a "licensed financial activity" in the UAE and which offer their products and services to consumers.

3.2.17 The Framework introduces key data protection principles which bring the new CBUAE Framework closer to international data protection standards. LFIs are required (among other things) to:

(a) *establish a department to oversee and manage the protection of consumer Personal Data;*

(b) *collect consumer Personal Data only to the extent required to allow LFIs to carry out their licensed activities;*

(c) *implement policies that specify the retention period of consumer Personal Data held by LFIs;*

(d) *implement appropriate security measures to detect, track and record unauthorised access to consumer Personal Data, and to prevent the misuse of consumer Personal Data;*

(e) *notify the CBUAE of all significant breaches affecting consumer Personal Data and, also, affected individuals if the breach poses a risk to their financial or personal security;*

(f) *obtain express (i.e. freely and explicitly obtained) consent of consumers before collecting, using and/or sharing their Personal Data;*

(g) *before obtaining their Personal Data, inform consumers in writing with respect to how their Personal Data will be processed;*

(h) *provide consumers with the right to withdraw their consent under certain circumstances, the right to request access to and correction of their Personal Data; and*

(i) *ensure that contracts with third parties contain appropriate provisions that restrict the sharing of Personal Data.*

3.2.18 Breaches of the Framework may be subject to supervisory action, which can lead to the CBUAE imposing sanctions and penalties, including fines or restrictions of power of LFI's senior management or board members. Sanctions can also be imposed by the CBUAE under the Decretal Federal

Law No. 14 of 2018 (the Banking Law), including imposing conditions or restrictions on the license of an LFI.

Central Bank Outsourcing Regulations

3.2.19 The CBUAE issued a formal set of Outsourcing Regulations and Outsourcing Standards for Banks (dated 31 May 2021) which aim to ensure that banks in the UAE are appropriately managing the risks when outsourcing certain functions.

3.2.20 The Outsourcing Regulations include data protection principles[58] which require banks to:

(a) *ensure compliance with all applicable UAE legislation and regulations in managing and processing data when outsourcing;*

(b) *retain ownership of all data provided to an outsourcing service provider, and ensure that their customers retain ownership of their data and can effectively exercise their rights and duties in this regard; and*

(c) *ensure that their data is secured from unauthorised access, including unauthorised access by the outsourcing service provider or its staff.*

3.2.21 Banks are also required to enter into outsourcing agreements which should contain the following:

(a) *the bank has full ownership of the data it shares with the service provider and that its customers retain full ownership;*

(b) *the bank has unfettered access to all of its data for the duration of the agreement and upon termination;*

(c) *appropriate provisions to protect a bank's data, including non-disclosure agreements and provisions related to the destruction of the data after termination of the agreement;*

(d) *establish standards for data protection, including any nationally recognised information assurance standards in the UAE; and*

(e) *no confidential data may be shared with any subcontractor without the prior specific authorisation of the bank or the customer, as the case may be.*

Telecommunications

3.2.22 The recently renamed The Telecommunications and Digital Government Regulatory Authority (**TDRA**) has implemented a number of regulations and policies that incorporate internationally recognised data protection principles.

[58] Article 4, Outsourcing Regulations

Internet Access Management Policy

3.2.23 The TDRA implemented the Internet Access Management Policy (the **IAM Policy**) in 2011, in coordination with National Media Council and Etisalat and Du, which are the licensed internet service providers in the UAE (the **Licensees**). The TDRA monitors online content available to users in the UAE and will bring any breaches of the IAM Policy to the attention of website operators.

3.2.24 Under the IAM Policy, online content that is used for impersonation, fraud and phishing and/or invades the privacy of individuals[59] can be reported to Etisalat and du to be taken down.[60] Content relating to the "invasion of privacy" includes: (i) internet content that allows access to private information illegally including those related to addresses and phone numbers of individuals or which disturbs individuals by way of spam messages; and (ii) internet content that exposes news, photos or comments related to the private or family life, even if it is true, if publishing such content may harm the concerned person.

Consumer Protection Regulations

3.2.25 The TDRA's Consumer Protection Regulations of 24 December 2015 impose a number of obligations on Licensees, the internet service providers licensed by the TDRA, when it comes to the handling of subscribers' information. These obligations include:

(a) *taking all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information;*

(b) *taking all reasonable measures to protect the privacy of subscriber information that is collected and maintained by the Licensees and using reliable security measures against risks such as loss or unauthorised access, destruction, leakage, inappropriate use, modification and unauthorised disclosure.*

(c) *limiting access to subscriber information to trained and authorised personnel, who are bound to protect the Licensee's confidential information from unauthorised use and disclosure under the terms of a written agreement, and adequately training such personnel;*

(d) *obtaining a subscriber's prior consent before sharing any subscriber information with affiliates and other third parties not directly involved in the provision of the telecommunications services ordered by the subscriber;*

[59] Annex 1 on Prohibited Content Categories, IAM Policy

[60] See User Privacy Protection section which requires website owners and internet services to provide privacy protections such as a privacy policy (https://www.tdra.gov.ae/en/about-tra/information-and-egovernment-sector/internet-guidelines/details.aspx#pages-67186)

(e) *where information is shared with third parties, ensuring that the third parties take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information and to use it only as required for the purposes of providing the telecommunication service; and*

(f) *ensuring that the contract between a Licensee and any affiliate or other third party holds that third party responsible for the privacy and protection of the subscriber information.*

IoT Policy

3.2.26 The Internet of Things (**IoT**) Regulatory Policy dated 22 March 2018 which regulates IoT services provided in the UAE (the **IoT Policy**), as issued by the TDRA, applies to Licensees, IoT service providers (i.e. any person that provides an IoT service to users) and IoT users.

3.2.27 The IoT Policy sets out a number of data protection principles which mirror the principles of international data protection laws, such as the GDPR. These principles include:

(a) "Purpose limitation*": Data should be collected through the IoT Service for specified, explicit and legitimate purposes only and not to be further processed in a manner that is incompatible with those purposes.*

(b) *"*Data minimisation*": Data should be limited to what is necessary in relation to the purposes for which it is processed.*

3.2.28 Moreover, the IoT Policy incorporates a data classification system consisting of four categories:

(a) *"*Open*": Data provided by individuals, businesses or the government to be freely or subject to a minimum limit, used or exchanged with third parties.*

(b) *"*Confidential*": Data, the unrestricted disclosure or exchange of which may cause limited damage to individuals, businesses or the government.*

(c) *"*Sensitive Data*": Data, the unrestricted disclosure or exchange of which may cause significant damage to individuals, businesses or the government.*

(d) *"*Secret*": Data, the unrestricted disclosure or exchange of which may cause significant damage to supreme interests of the country and very high damage to individuals, businesses and the government.*[61]

[61] Section 7.8.2.1 of the IoT Policy further states that any "Personal Data" [61] is deemed by the TDRA to be "Secret" data for individuals.

3.2.29 The IoT Policy requires Secret, Sensitive and Confidential data for individuals and businesses to be stored within the UAE.[62] Such data may be stored outside the UAE provided that the destination country for data storage meets or exceeds any data security and user protection policies/regulations followed within the UAE.[63] These conditions also apply to Personal Data. If the destination country can be shown to meet or exceed UAE data security and consumer protection regulations, then the data localisation requirement will not apply to such data.

3.2.30 The IoT Policy also considers "*not implementing the defined **consent** administration for **Data Processing***" (emphasis as set out in the IoT Policy) to be a violation. However, the IoT Policy does not specify in the main body of the policy that such specific consent should be obtained. It does define "Consent" to be "*any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to Data Processing for data relating to them*". It is likely that this implies that IoT Service Providers should obtain "*freely given, specific, informed*" consent from users.

3.2.31 Service providers of IoT therefore have to comply with the data protection standards set out in the IoT Policy. Non-compliance with any of the provisions of the IoT Policy will be considered a breach of the UAE Telecom Law.[64] The TDRA will report such a breach to concerned authorities. Breaches of the UAE Telecom Law could expose a service provider to fines of up to AED 1,000,000 (approx. GBP 200,000).[65]

3.3 Dubai Emirate-level laws

3.3.1 Alongside UAE federal laws and regulations, the Emirate of Dubai has also developed laws that apply principles of privacy and data protection as seen in international data protection legislation, such as the GDPR.

Dubai Data Law

3.3.2 Dubai Law No. 26 of 2015 regulating data dissemination and exchange in the emirate of Dubai (**Dubai Data Law**) and its accompanying policies and standards (**Dubai Data Policies**) include specific requirements to protect Personal Data. It is monitored and enforced by Smart Dubai, the government department that was established to empower, deliver and promote an efficient, seamless, safe and impactful city experience for residents and visitors.

3.3.3 The Dubai Data Law is aimed primarily at ensuring that data gathered by Dubai government entities is effectively shared amongst such entities and

[62] Section 7.8.2.1, the IoT Policy
[63] *Ibid*.
[64] Section 9.5, IoT Policy
[65] Article 74, Telecom Law

with the private sector. The Dubai Data Law defines 'Dubai Data' as "*data which is available to data providers [i.e. federal government entities, local government entities and other parties determined by Smart Dubai as the entity responsible for supervising the implementation of the law] and is related to the Emirate*". The Dubai Data Law aims to establish controls around such Dubai Data.

3.3.4 One of the purposes of the Dubai Data Law includes managing data in conformity with international best practices, promoting transparency and establishing rules for data dissemination and exchange, increasing the efficiency of services provided by federal government entities and local government entities, and providing data necessary to non-governmental entities with a view to supporting the development of the Emirate of Dubai. The Dubai Data Law seeks to strike a balance between data dissemination and exchange, and data confidentiality and privacy.

3.4 Federal and local cyber/data policies and strategies

Federal Information Security Resolution

3.4.1 All Federal entities within the UAE including ministries, public corporations, institutions and public bodies are legally required to enforce Information Security policies since the introduction of the UAE Cabinet Resolution No. 21 of 2013 (**FIS Resolution**).

3.4.2 The FIS Resolution is aimed at managing the data security environment in the federal government. It provides a legal framework for information security and requires IT departments to enforce security policies to protect their critical data and control its use and movement. One way the FIS Resolution seeks to enforce these obligations is by requiring federal employees to classify all data assets processed by the public entity.

3.4.3 Every federal employee is legally liable for non-compliance with the FIS Resolution and is required to sign an acknowledgment to this effect. Failure to comply could mean fines or even imprisonment for employees.

3.4.4 Additionally, the FIS Resolution expressly states that "*every User (who) violates the provisions of this Regulation shall be punished according to the disciplinary sanctions set forth in the human resources laws and regulations applied in the FE he/she works for*". Accordingly, employees found not to be complying with the FIS Resolution are subject to internal disciplinary regulations and penalties set by their employers in addition to any civil sanctions or imprisonment.

UAE Cybersecurity Council

3.4.5 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 resilient cyber infrastructure in the UAE.

National Cyber Security Strategy

3.4.6 The TDRA developed the UAE National Cyber Security Strategy in 2019 with the aim of creating a resilient cybersecurity infrastructure in the UAE.

3.4.7 The Strategy was developed based on the analysis of more than 50 sources of indicators and international publications, in addition to working with a team of international experts and benchmarking with 10 leading countries in cybersecurity systems. It is based on 60 initiatives across five pillars, including:

(a) *Cybersecurity laws and regulations: The Strategy aspires to create a legal and regulatory framework to address all types of cybercrimes and to secure existing and emerging technologies. The UAE government aims to achieve these aims through the development of various laws, including data protection and privacy laws.*

(b) *National Cyber Incident Response plan: The Strategy aims to streamline cybersecurity incident detection and reporting and to build world-class capabilities to respond to all types of cyber incidents.*

3.4.8 In January 2021, the UAE government announced that it would be updating the Strategy in line with rapid technological developments since the Covid-19 pandemic.

UAE Information Assurance Regulation and Standards

3.4.9 The TDRA also implemented the National Information Assurance Regulation (**IA Regulation**) and National Information Assurance Standards in 2020 to align with the National Cyber Security Strategy and to reflect the UAE government's commitment to the development of a secure national information and communications infrastructure for UAE organisations and individuals. The aim of the IA Regulation is to provide requirements to raise the minimum level of protection of information assets and supporting systems across all implementing entities in the UAE.

3.4.10 The IA Regulation is based on regional and global best practices including ISO 27001, COBIT, NIST, SANS and Abu Dhabi Systems and Information Centre (ADSIC).

3.4.11 The Standards are a set of 188 standards, security controls and guidelines for government entities in critical sectors. Compliance with these standards is

mandatory for all government organisations, semi-government organisations and business organisations that are identified as critical infrastructure to UAE. The Standards cover a broader range of information protection and management aspects including business information continuity, disaster recovery, compliance, certification and accreditation.

National Cyber Risk Management Framework

3.4.12 The National Cyber Risk Management Framework is a framework for identifying, assessing, treatment planning, monitoring and communicating critical national and sector-level cyber security risks.

National Cyber Information Policy

3.4.13 The National Cyber Information Policy outlines key requirements for inter-entity and inter-sector communication that serves as a key input to developing national situational awareness.

Dubai Cyber Security Strategy

3.4.14 In addition to the federal cybersecurity strategies and policies, Dubai has also implemented a Strategy for 2021 that sets the Dubai government's objectives towards enhancing cybersecurity in the Emirate. In line with the Strategy, Dubai has developed its own standards, including the IoT Security Standard and Cloud Service Provider Security Standard.

3.4.15 The Dubai government also founded the Dubai Electronic Security Center (DESC) pursuant to Dubai Law No. 11 in 2014 with the aim to develop and implement information security practices and set good-practice criteria for cyber security, across the Emirate.

Part 3: Legal Framework – DIFC Data Protection Law and Regulations66

4 Principles for Processing Personal Data

4.1 Internationally recognized data protection principles and guidelines

4.1.1 The principles for processing Personal Data set out in the DIFC DPL are all comparable to internationally recognized data protection laws and guidelines such as the OECD Convention 108+, internationally recognized data protection laws such as the GDPR and UK GDPR, and the laws of Colombia. Please see below for details.

4.2 Compatibility of the DIFC DPL principles with similar laws

4.2.1 The following comparison table provides information about the compatibility of the DIFC DPL principles with similar laws:

Content principles - based on OECD guidelines / Convention 108, as well as enshrined in globally recognized frameworks (i.e., the GDPR / UK GDPR)	**Exists in DIFC DPL / Explanation**
Existence of basic definitions and principles - basic data protection definitions and principles should exist. They should reflect and be consistent with the concepts enshrined in commonly accepted data protection laws. For example, the GDPR includes the following important concepts: “Personal Data”, “processing of Personal Data”, “data Controller”, “data Processor", “recipient” and “sensitive / Special Category Data”.	YES – Please see Schedule 1, Article 3 Definitions - all relevant, common definitions present in DIFC DPL, equivalent across comparable laws, and related Guidance
Grounds for lawful, fair processing for legitimate purposes - Data must be processed in a lawful, fair and legitimate manner. The legitimate bases, under which Personal Data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. There are several such legitimate grounds including for example, provisions in national law, the consent of the Data Subject, performance of a contract or legitimate interest of the data Controller or of a third party which does not override the interests of the individual.	YES - Articles 9 to 13, particularly Article 12 re: consent, and related Guidance

[66] Guidance on all topics is available here: https://www.difc.ae/business/operating/data-protection/guidance/

Content principles - based on OECD guidelines / Convention 108, as well as enshrined in globally recognized frameworks (i.e., the GDPR / UK GDPR)	**Exists in DIFC DPL / Explanation**
Purpose limitation principle - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the listed grounds.	YES - Article 9 provides primary principles. In addition, the DIFC DPL adds requirements for specific information to be provided to Data Subject regarding type of technology to be used for processing, and other changes in processing set out in Article 29(1)(h)(ix), and related Guidance
Data retention principle - data should, as a general rule, be kept for no longer than is necessary for the purposes for which the Personal Data is processed	YES - Article 9 and related Guidance
Data quality and proportionality principle - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed	YES - Article 9 and related Guidance
Transparency principle -Each individual should be informed of all the main elements of the processing of his/her Personal Data in a clear, easily accessible, concise, transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data Controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest.	YES - Articles 12, 29 and 30, and related Guidance
Security and confidentiality principle - technical and organisational security measures should be taken by the Controller that are appropriate to the risks presented by the processing. A Processor, must not process data except on instructions from the Controller	YES - Article 9, as well as Part 7 of the DIFC DPL and related Guidance

5 Rights of Data Subjects

5.1 Comparable Data Subjects' rights and protections

5.1.1 Obligations for protection the rights of Data Subjects are set out as follows:

Rights of access, rectification, erasure, objection, portability The Data Subject should have the right to obtain confirmation about whether or not data processing concerning him / her is taking place as well as access his/her data, including obtaining a copy of all data relating to him/her that are processed. The Data Subject should have the right to obtain rectification of his/her data as appropriate, for example, where they are inaccurate or incomplete and erasure of his/her Personal Data when, for example, their processing is no longer necessary or unlawful. The Data Subject should also have the right to object on compelling legitimate grounds relating to his/her particular situation, at any time, to the processing of his/her data under specific conditions established in the third country legal framework. For example, such conditions include when the processing is necessary for the performance of a task carried out in the public interest or when it is necessary for the exercise of official authority vested in the Controller or when the processing is necessary for the purposes of the legitimate interests pursued by the data Controller or a third party. The exercise of those rights should not be excessively cumbersome for the Data Subject. Possible restrictions to these rights could exist for example to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest.	YES - Article 9 and Part 6 Any limited restrictions to such rights covered in Article 33 primarily. Articles 34 to 38 cover the right to object, restrict, rectify, port / freely move data to new providers, and rights regarding automated decision making, as per the GDPR and UK GDPR (almost verbatim) DIFC DPL also incorporates a very useful non-discrimination clause at Article 39.

5.2 Guidance and assessment tools

5.2.1 The Data Protection webpage contains a Guidance sub-menu available at this link. The Commissioner's Office also has extensive, specific information set out on the Accountability and Rights sub-menu of the Data Protection website.

6 Legal Duties of Controllers and Processors

6.1 Accountability and compliance requirements

6.1.1 The legal duties of Controllers and Processors is set out primarily in Parts 2 and 3 of the DIFC DPL, regarding accountability and compliance requirements, appointing data protection officers, conducting annual assessments and data protection impact assessments, and cessation of processing.

6.1.2 Also covered are contractual obligations of Controllers and Processors, limitations and safeguards for transfers of Personal Data outside of the DIFC, and government authority access to data. The latter is covered in Article 28, and an MOU template for the purposes of written assurances prescribed under Article 28 is available at this link and in Appendix C. All such obligations are again as per the GDPR and the UK GDPR, and further guidance can be found as follows:

6.2 Guidance and support for Accountability matters

General guidance:
https://www.difc.ae/business/operating/data-protection/guidance/

Accountability and Individual Rights:
https://www.difc.ae/business/operating/data-protection/accountability/

Data Export and Sharing:
https://www.difc.ae/business/operating/data-protection/data-export-and-sharing/

Personal Data Breach Reporting:
https://www.difc.ae/business/operating/data-protection/security-breach-reporting/

6.3 Legal duties of Controllers and Processors

Restrictions on onward transfers Further transfers of the Personal Data by the importer of the original data transfer should be permitted only where the further recipient (i.e., the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data Controller. The level of protection must not be undermined by the onward transfer. The initial importer of the shared data shall be liable to ensure that appropriate safeguards are provided for onward transfers of data. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.	YES - Articles 26 and 27

Additional safeguards for processing special categories of Personal Data Specific safeguards should exist where 'special categories' of data are involved. This protection should be achieved through more demanding requirements, such as explicit consent.	YES - Article 11, Article 12, Article 28
Affirmative choices in direct marketing and electronic communications Where data are processed for the purposes of direct marketing, the Data Subject should be able to object without any charge from having his/her data processed for such purposes at any time.	YES - Articles 29 and 34, and Direct Marketing Guidance
Good level of compliance with the rules A good system is generally characterised by a high degree of awareness among data Controllers of their obligations, and among Data Subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials	Guidance and FAQs available on DIFC website - https://www.difc.ae/business/operating/data-protection/faqs-glossary/ Inspections / Supervisory visits conducted regularly (100 per year, as time and schedules permit) Sanctions issued for failure to re-notify the Commissioner and various breaches of the DP Law, set out in Schedule 2 of DP Law
Accountability A third country data protection framework should oblige data Controllers and/or those processing Personal Data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.	YES - Articles 14 to 22 and related Guidance https://www.difc.ae/business/operating/data-protection/guidance/#s12

Part 4: Data sharing / Government information requests

7 Overview of Government information requests in the UAE

7.1 Establishment and powers of UAE government authorities

7.1.1 Each ministry and government authority in the UAE is established by federal law which prescribes the powers that such authority will have and the areas in which it can regulate. Article 58 of the UAE Constitution states that: "*The law shall determine the jurisdiction of the Ministries and the powers of each Minister*". Additionally, under Federal Law No. 1 of 1972, "*Each Federal Ministry shall carry out the competences entitled thereto by virtue of the present law, as well as the other federal laws, regulations and rules, issued by virtue of the provisions of the Constitution*".[67]

7.1.2 Federal ministries are also required to practice their powers in line with the guidelines of the Cabinet and the federal laws.[68] By way of example, the National Media Council was established by virtue of Article 4 of the Federal Decree Law No. 11 of 2006 (**NMC Law**) as the federal government body entrusted to oversee and undertake the media affairs in the UAE, both onshore and in the free zones. The National Media Council carries out the competencies set for the Ministry of Information and Culture. The NMC Law sets out the specific powers of the National Media Council and its responsibilities in relation to supervising media in the UAE.[69] It provides the National Media Council with all necessary legal capacity to carry out all actions and dispositions that could achieve the objectives of the NMC Law.

7.1.3 Each ministry and government authority's powers, therefore, are limited to those powers prescribed by the federal law that established them.

7.2 Government data sharing in the DIFC

7.2.1 DIFCA has developed an internal DIFC policy that governs fair and lawful sharing of Personal Data requested by government entities within the UAE and elsewhere (the **DIFC Government Data Sharing Policy**).[70] This has largely been developed from the principles introduced in Article 28 of the DIFC Data Protection Law No.5 of 2020, which set out a data sharing assessment model (as described in further detail below).. AWS adopted an approach of challenging law enforcement requests for customer data from governmental bodies where such requests conflict with legislation, are overly broad or otherwise where AWS has grounds to do so.[71] The DIFC DPL obliges Controllers to undertake similar assessments of governmental data requests.

[67] Article 1, Federal Law No. 1 of 1972
[68] Article 20, Federal Law No. 1 of 1972
[69] Article 5, NMC Law
[70] See 0
[71] https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

7.2.2 To fully implement the DIFC Government Data Sharing Policy, DIFCA has executed Memoranda of Understanding (**MOU**) for data sharing with at least two (2) UAE authorities from which it typically receives the majority of data requests, with others in train. The template MOU[72] references Article 28 of the DIFC DPL directly, acknowledging that both parties will implement appropriate measures as set out in the legislation to ensure the security of Personal Data obtained or processed. The underlying purpose of the MOU is to highlight legal obligations applicable to Personal Data processed in the DIFC to government authorities that may not otherwise be familiar with the same.

7.2.3 Prior to the introduction of Article 28 by way of the DIFC DPL, DIFCA agreed data sharing agreements espousing the same principles and requirements with the Dubai Financial Services Authority (**DFSA**), another DIFC Body, as well as various MOUs for certain purposes with government entities including Dubai Statistics Centre, Dubai Economic Department, the UAE Ministry of Economy and the UAE Ministry of Finance. Each of these MOUs included robust data protection clauses. The general MOU being executed at this time covers any engagement.

7.3 Government requests to DIFC Controllers and Processors

7.3.1 While government authorities have powers prescribed to them by Federal laws, there are protections set out in the DIFC DPL in relation to the sharing of Personal Data by DIFC Controllers or Processors with government authorities under Article 28 thereof.

7.3.2 Where a Controller or Processor receives a request from any public authority, whether in the UAE or outside the UAE, for the disclosure and transfer of Personal Data, it must carry out the certain procedures outlined in Article 28 and set out in more detail below.

7.3.3 As a Controller itself, and a government entity, DIFCA routinely receives information sharing requests for a variety of purposes. As noted previously, DIFCA has engaged in constructive discussion with these organisations to assure proper implementation of the above requirements through any data sharing environment. UAE government authorities appear willing and ready to take on principles and obligations that support building an ethical data sharing culture.

7.3.4 Controllers and Processors (upon reasonable notice to the Controller) may disclose or transfer Personal Data to the public authority as long as they have taken reasonable steps to ensure that the request from the public authority is

[72] See DIFC Export and Sharing webpage for the MOU template.

valid and proportionate and the public authority will respect the rights of Data Subjects when processing any Personal Data shared to it by the Controller.

7.3.5 Accordingly, if a (UAE or Dubai) government authority makes a request that involves the sharing of Personal Data, then such a request must take into account the framework of obligations set out in the DIFC DPL. All entities in the DIFC have to make an assessment in line with Article 28 as outlined above before sharing any Personal Data with such authorities and all such authorities should recognise the legal basis of the DIFC DPL given that it ultimately derives from constitutional powers and appointments.

7.3.6 Information and guidance about Article 28 is found at here and here. An Article 28 assessment tool is available at this link.

8 UAE public authorities' access to Personal Data transferred from DIFC

8.1 Federal and Local laws impacting public authority access to DIFC private entity Personal Data

8.1.1 On the federal level, laws regulating different sectors may set out, where necessary, the powers of public authorities to procure and process data in relation to such sector.

8.1.2 Additionally, powers of public authorities to process data may be based on the laws establishing public authorities, as such laws would explicitly set out the powers and duties of the concerned public authority. In either case, the type of data that the public authority is able to collect would be limited to the sector or subject matter that the public authority regulates and would be subject to the protocols and safeguards set out in more detail below.

8.1.3 Additionally, UAE federal criminal laws criminalize and sanction acts of illegal access to or misuse of data, providing an additional layer of protection; ensuring compliance with the law and preventing illegal access or processing of Personal Data by all individuals, including public authorities' employees.

8.1.4 On a local Emirate level, the government of Dubai issued multiple laws in recognition of the importance of governance of data dissemination and exchange. These laws apply to federal and local government authorities based in Dubai as well as private entities viewed as data providers, including those based in the DIFC.

8.2 Relevant Federal and local laws:

Relevant Federal Laws:	Relevant local laws include:

- Federal Law No (14) of 2018 regarding the Central Bank and Organization of Financial Institutions and Activities and its amendments; - Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the AML Law) and its amendments; - Federal Law by Decree No. (3) of 2003 Regarding the Organization of Telecommunications Sector and its amendments; - Federal Law No. (2) of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Fields; - Federal Decree-Law No. (31) of 2021 issuing the Crimes and Penalties Law and its amendments ("Crimes and Penalties Law"); and - Federal Decree Law No. (34) of 2021 on Combatting Rumours and Cybercrimes ("Cybercrimes Law") . - Federal Decree Law No. (46) of 2021 on Electronic Transactions and Trust services.	- Law No. (26) of 2015 regulating Data Dissemination and Exchange in the Emirate of Dubai ("Dubai Data Law") . - Resolution No. (2) of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai ("Dubai Data Policies") .

9 Limitations and Safeguards

9.1 In DIFC laws regarding Personal Data sharing by DIFC entities with *any* public authorities

9.1.1 While government authorities have powers prescribed to them by federal and emirate laws, as summarized above, the protections set out in the DIFC DPL in relation to the sharing of Personal Data by DIFC Controllers or Processors with any government authorities under Article 28 would apply to requests made by non-DIFC, UAE-based public authorities.

9.1.2 Article 28 imposes the data protection equivalent of enhanced due diligence that is common to laws such as those addressing anti-money laundering and countering terrorism. The enhanced due diligence obligations under Article

28 require any DIFC entity processing Personal Data to assess government data sharing requests against additional risks and their impact and to determine the necessity and proportionality of the request. Where possible, written assurances through an MOU or other written agreement are an additional safeguard akin to the standard contractual clauses for general international transfers. Please refer to the DIFC DPL Article 28 guidance, FAQs and assessment tool for further information.[73]

9.1.3 DIFC DPL demonstrates its safeguards and controls when sharing Personal Data with federal or emirate government authorities, Article 28 states the following:

"(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it should:

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;

(b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-Processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

[73] DIFC Data Protection Guidance webpage

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28."

Additionally, the President of the DIFC, Sheikh Maktoum Bin Mohammed Bin Rashid AlMaktoum, issued Presidential Directive No 4 of 2022 ("Directive 4")[74] emphasizing that Article 28 of the DIFC DPL applies to all requests from public authorities for Personal Data from DIFC private entities, and providing further detail on the applicability and assurances relating to relevant articles of the DIFC DPL regarding request for sharing personal Data with a public authority.

9.2 In UAE regulations

9.2.1 UAE law criminalizes and sanctions in different criminal laws acts involving illegal disclosure or misuse of data, setting higher sanctions in certain cases upon public servants to safeguard Data Subjects from any data misuse by public authorities employees and ensure compliance with the relevant laws and regulations.

9.2.2 For example, Article (296) of the Crimes and Penalties Law provides that:

"A penalty of temporary imprisonment shall be imposed on any public servant or any person entrusted with a public service, apart from those mentioned in the preceding Article, who gives, damages, conceals, or facilitates for another person the acquisition of, information or data that he knows of or unlawfully extracts by virtue of his office".

9.2.3 Furthermore, the Cybercrimes Law includes further provisions that criminalize and sanction non-compliance with Personal Data protection rules in force by any individual, including public authorities' employees, as it stipulates in Article (13) that:

"Whoever uses the information technology or ITE to collect, save, or process Personal Data and information of nationals and residents of the UAE in violation of the legislation in force in the UAE shall be punished with

[74] Directive 4 is available on the DIFC Data Protection Supervision and Enforcement webpage

imprisonment and/ or a fine of not less than (AED 50,000) fifty thousand dirhams or more than (AED 500,000) five hundred thousand dirhams."

9.2.4 Additionally, the Cybercrimes Law criminalizes and sanctions illegal interception and disclosure of information, as it provides in Article (12) that:

"1. Whoever obstructs or intercepts the access to an information network, website, or electronic or any electronic connection, information or data shall be punished with imprisonment and/ or a fine of not less than (AED 150,000) one hundred fifty thousand dirhams or more than (AED 500,000) five hundred thousand dirhams.

2. If the offender discloses or leaks the information, data or purport of the communication obtained through the interception shall be punished with imprisonment for at least one year and fine of not more than (AED 1,000,000) one million dirhams.

3. If the interception involves the communication, information or data of one of the government entities, the penalty shall be temporary imprisonment."

9.3 In local (Emirate) laws and frameworks

9.3.1 In recognition of the importance of data protection, the Dubai Data Law, through Articles (9) and (12) highlights the legal requirement for compliance by Federal and Local Government Entities, as well as Private Entities where they are viewed as a data provider, with the rules, standards and conditions set out by the Competent Authority. Dubai Data Policies as approved by Resolution No. (2) of 2017 elaborate on this by providing further detail on the rules, standards and conditions referred to in the Dubai Data Law.

9.3.2 Article (21) of the Dubai Data Policies highlights the need for special attention in relation to Personal Data as it provides that :

A. "The entities and Persons governed by this Document must not disclose, or otherwise classify as Open Data and disseminate, any Personal Data, Private Entities' Data, or Private Entities' Sensitive Data.

B. In the course of implementing the Data Classification Process, a Data Team must identify Personal Data, Private Entities' Data, and Private Entities' Sensitive Data which may not be included in an Open Data Set. In any event, Dubai Data may not be classified as Open Data until all restricted Data, as per the classification, is removed."

9.3.3 Article (23) of the Dubai Data Policies then sets out explicitly the requirement for consent and respect of data protections principles, such as transparency, purpose limitation, and data minimisation, providing that:

"A Government Entity must:

1. seek the consent of individuals and Private Entities to use, store, process, and exchange with other Government Entities in the Emirate their Personal Data, Private Entities' Data, or Private Entities' Sensitive Data to enable any Government Entity to provide services to its customers without the need to request the same Data again;

2. obtain the consent of the relevant Intellectual Property Rights holder, where it is commercially viable for both the rights holder and the Government Entity, to use or reproduce protected Data for the purpose of the Government Entity providing its services to its customers;

3. provide options for individuals and Private Entities to amend their Data or revoke their consent on exchanging their Data among Government Entities;

4. adhere to the following principles, when handling Personal Data, Private Entities' Data, or Private Entities' Sensitive Data; or granting Access Permissions related thereto:

a. Transparency: by informing individuals and Private Entities of which Government Entity will collect their Personal Data or private Data.

b. Purpose: by using the collected Data for specific and explicitly stated purposes.

c. Proportionality: by ensuring that the type of Data collected is the minimum required to achieve the purpose for which it is collected".

9.3.4 Additionally, Article (13) of the Dubai Data Law affirms the importance of data protection as it sets out that:

A. "The provisions of this Law are without prejudice to the rules, scope, and cases of legal protection under the Data legislation in force, regardless of the type, nature, or form of Data.

B. Data Providers must, in the course of Data dissemination and exchange, take all the procedures required for the protection of the confidentiality and privacy of legally protected customer Data."

9.3.5 The above mentioned legal provisions apply to Federal and Local Government Entities, as well as Private Entities viewed as a data provider, where they hold or process Dubai Data.

9.3.6 It is also beneficial to understand that the Dubai Data Policies introduce the Dubai data classification principles, upon which different data exchange standards would apply to different types of data. As data classification principles and data exchange standards in Dubai are aligned with the federal standards, the document will continue to highlight such standards as they are adopted at the UAE level by the UAE Smart Data Framework. Details about the Smart Data Framework are set out in Appendix B.

9.4 Data Subjects' rights and oversight / redress where UAE public authorities access Personal Data

9.4.1 Article (41) of the Constitution stipulates that: "*Every person shall have the right to submit complaints to the competent authorities, including the judicial authorities, concerning the abuse or infringement of the rights and freedoms stipulated in this Chapter*". Such rights include the rights to secrecy and privacy (Article 31 and Article 36).

9.4.2 Individuals have the power to seek redress from government authorities in the UAE in addition to any remedies available under UAE federal and Emirate laws relating to privacy and data protection against entities that violate such laws.

9.4.3 Judgments brought by individuals and/or companies can generally be enforced against UAE government entities (including regulatory authorities).

9.4.4 UAE law does not grant state entities immunity from suit. Accordingly, government entities can be sued. However, Article 242 of UAE Federal Decree-Law No. 42 of 2022 (the Civil Procedures Law) includes a general prohibition on the seizure of "public property owned by the state or any of the Emirates" for the purposes of enforcement.[75]

9.4.5 Upon receiving a final judgment against UAE regulatory authorities (i.e. Central bank, Securities and Commodities Authority, Dubai Financial Services Authority in DIFC), it is mandatory to obtain a permission from the Ruler's court to enforce the judgement against the above-mentioned authorities according to the following procedure:

(a) *the Claimant must complete the "Complaint against Government Entities Form" accompanied by a statement of claim and relevant supporting documents, either through the smart App or the Department of Legal Affairs' (the **Department**) website;*

[75] Civil Procedures Law

(b) *within one week of receiving the complaint, the Department will send the statement of claim and any supporting documents to the relevant Government entity, requesting their legal commentary and feedback within fifteen days from the date of receipt; and*

(c) *after receiving the Government entity's feedback, the Department will seek to settle the dispute amicably. If two months have passed since the filing of the claim without reaching an amicable end of the dispute, the complainant may resort to the competent judicial authority to commence proceedings.*

9.5 Data Sharing with respect to international co-operation commitments

9.5.1 There are a range of compliance obligations imposed on the DIFC as a jurisdiction by the Organisation for Economic Co-operation and Development (OECD) and other international bodies to ensure the safe automatic exchange of information (AEOI).[76] The DIFC has implemented several measures to assure safeguards for these laws, which have been approved by UAE authorities. Specific examples of international co-operation include recently-introduced UAE legislation on economic substance, tax evasion and money laundering. For example, as recommendations and new UAE regulations are being implemented regarding Economic Substance and Common Reporting Standard reporting, the UAE Ministry of Finance required DIFC complete an AEOI questionnaire in December 2020 (at the direction of the OECD). The questionnaire set out DIFCA's privacy and security framework generally, specifically pointing out measures in place to safeguard highly sensitive data where sharing for the purposes of regulatory enforcement was required.

Economic substance

9.5.2 The Economic Substance Regulations (Cabinet of Ministers Resolution No. 31 of 2019) (**ESR**) were issued in April 2019 and provide an example of a federal law that has followed international practice. The UAE Ministry of Finance (**MOF**) confirmed that it had introduced ESR as part of its commitment as a member of the OECD Inclusive Framework and in response to an assessment of the UAE's tax framework by the EU Code of Conduct Group on Business Taxation.[77]

9.5.3 The purpose of ESR is to ensure that UAE entities report actual profits that are commensurate with the economic activity undertaken within the UAE. The ESR require UAE onshore and free zone companies and certain other business forms that carry out any "Relevant Activities" to maintain and demonstrate an adequate "economic presence" in the UAE relative to the activities they undertake (by way of an economic substance test).

[76] See details on the AEOI standard here: https://www.oecd.org/tax/transparency/what-we-do/
[77] See: https://www.mof.gov.ae/en/strategicpartnerships/pages/esr.aspx

9.5.4 The ESR require corporate entities and partnerships undertaking relevant activities in the UAE to file a notification containing information in respect of the licensee and their activities. The content of the notification, means of filing and the purposes for which the notification is filed are all set out in MOF guidance.[78] Similarly, there is guidance on the content and purposes of the economic substance report that qualifying entities must submit.[79] The MOF website also outlines why the UAE introduced the ESR, the identity of all relevant regulatory authorities, the scope of application of the ESR and contact details for all regulatory authority designated contacts.

Common Reporting Standard

9.5.5 The OECD together with G20 countries, and in close cooperation with the EU and other stakeholders, developed the "Standard for Automatic Exchange of Financial Account Information" or "the Standard". This is a standardised automatic exchange model prepared to maximise efficiency of reporting and punitive measures.

9.5.6 In 2015, the UAE enacted Common Reporting Standard Regulations (**UAE CRS**) that applies in all UAE jurisdictions, including financial free zones such as the DIFC. DIFC subsequently enacted the Common Reporting Standards Law, DIFC Law No. 2 of 2018 (the **DIFC CRS Law**) in relation to the information gathering and reporting obligations imposed on Reporting Financial Institutions (**RFIs**) under the DIFC CRS Law and the Common Reporting Standards Regulations 2018 (the **Regulations**) (together, the **DIFC CRS**).

9.5.7 Penalties, enforcement and appeals are set out in Part 4 of the DIFC CRS Law, and Schedule 2 includes a list of fines and other disciplinary actions. As such, enforcement may include reporting non-compliance to competent authorities within and outside of the UAE. As such, per the DIFC CRS, DIFCA will in certain cases exchange information with MOF, which will then follow its own procedures for exchange of information with Participating Jurisdictions.

AML, financial crime and trafficking

9.5.8 The UAE issued Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the **AML Law**)[80] to align the UAE financial sector with international best practices on financial crime prevention.

[78] See: https://www.mof.gov.ae/en/StrategicPartnerships/Documents/Economic%20Substance%20-%20Notification%20Guidance.pdf
[79] See: https://www.mof.gov.ae/en/StrategicPartnerships/Documents/Economic%20Substance%20-%20Economic%20Substance%20Report%20Guidance.pdf
[80] https://www.mof.gov.ae/en/lawsAndPolitics/govLaws/Documents/EN%20Final%20AML%20Law-%20Reviewed%20MS%2021-11-2018.pdf

9.5.9 The AML Law introduces a number of concepts recommended by the UAE Financial Action Task Force, which are designed to enhance UAE's effectiveness in identifying and preventing attempts at money laundering and terror financing.

9.5.10 The right of access to accounts, records and documents is given to the public prosecution "*sua sponte or upon the request of the law enforcement authorities*" with a further right to request direct access to stored data if there is sufficient evidence of the occurrence of the crime.[81]

9.5.11 The Financial Intelligence Unit of the Central Bank to which suspicious transaction reports and information on financial institutions must be sent for consideration and (where necessary) referral to the competent authorities is responsible for the exchange of information with counterparts in other countries "*according to international agreements to which the State is a party or bilateral agreements signed by the FIU with its counterparts governing bilateral cooperation or conditional upon reciprocity*".[82] The AML Law includes a requirement that the information is only used for the purposes of combating the crime and shall not be disclosed to third parties without the Unit's permission. There is also a specific obligation "*to implement data privacy and data security procedures to protect this information including procedures for handling, archiving transferring and accessing the data, and make sure that access to its premises, its database and its technology systems is restricted*".[83]

10 Safeguards between DIFC and UAE Public Authorities

10.1 Engagements with non-DIFC authorities

10.1.1 The DIFC Bodies are taking numerous steps to reinforce the important principles of data protection not only in the DIFC but throughout the UAE and the wider region of Gulf Co-Operation Council (**GCC**)[84] states. DIFC aims to lead in the space of cultural change to support privacy and security from an accountability perspective, starting with its engagements with other government entities and regulatory authorities throughout the region.

10.1.2 Through these engagements, DIFC reinforces the important concept that government access to Personal Data must be proportionate, lawful and targeted.

[81] Article 7(1), AML Law
[82] Article 9(1), AML Law
[83] Article 9(3), AML Law
[84] The Cooperation Council for the Arab States of the Gulf is a regional, intergovernmental political and economic union consisting of the UAE, the Kingdom of Bahrain, the State of Kuwait, the Sultanate of Oman, the State of Qatar and the Kingdom of Saudi Arabia.

10.2 Requests from non-DIFC bodies

Training and culture of DIFCA staff

10.2.1 As mentioned, DIFCA maintains and implements a Government Data Sharing policy that incorporates the principles of Article 28 of the DIFC DPL. DIFCA staff, including new joiners, receive training on it regularly, and DIFC share it as needed with other government authorities to support the execution of the types of agreements mentioned in Article 28.

Vetting data sharing requests

10.2.2 Actions required when reviewing and responding to a government authority data sharing request are set out in the Government Data Sharing Policy. Generally, any DIFCA employee who receives such a request forwards it to the Director of Data Protection for review and approval.

10.2.3 Any queries are discussed with the relevant authority.

10.2.4 All requests that are challenged by the requesting authority are reviewed and assessed by the Director of Data Protection and may be escalated to Commissioner of Data Protection.

10.2.5 Data protection impact assessments are conducted as needed, including for any engagement in collaborative UAE programmes that require information sharing.

10.2.6 Records of data sharing requests maintained by relevant department receiving the request.

10.3 MOUs and other binding agreements

Updating existing MOUs and agreements

10.3.1 In addition to the Government Data Sharing Policy, any existing MOUs or inter/intra-government agreements with government authorities are updated when renewed to include data protection/Article 28 clauses and requirements.

10.3.2 Part of this engagement naturally results in an opportunity to update and clarify to non-DIFC authorities the importance of including and implementing data protection principles in all sharing activities.

New MOUs

10.3.3 Where no such MOU exists, a new MOU is executed specifically around government data sharing requirements under Article 28 of the DIFC DPL. As at the date of this memorandum, several MOUs are being reviewed and executed with key UAE authorities with whom the DIFC shares Personal Data.

Part 5: Independent Authority and Powers

11 DIFC Commissioner of Data Protection

11.1 Independent, competent public authority

11.1.1 The Commissioner of Data Protection is the competent, public authority in charge of supervising the processing of Personal Data in the DIFC.

11.2 Commissioner's powers and functions

11.2.1 Further details about the Commissioner's powers and functions are provided below:

Competent Independent Supervisory Authority / support and help to individual Data Subjects The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints. One or more independent supervisory authorities, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations.	DIFC DP Law contains: Supervisory Authority - DIFC Data Protection Commissioner - Part 8 Complaints and investigations mechanisms - Part 9, DIFC DP Law Sanctions and fines imposed - Part 9, DIFC DP Law Remedies available - Part 9, DIFC DP Law Notification requirements - Article 14, DIFC DP Law
Appropriate redress to the injured party where rules are not complied with This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate. The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to	In addition to the powers of investigation, taking complaints and mediation of the Commissioner, DIFC Courts and appeals mechanism for breach, allows for compensation to be paid; additionally, the Commissioner can make and issue decisions, orders, sanctions, etc. See above for further powers details.

ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice. Where rules are not complied with, the Data Subject should be provided as well with effective administrative and judicial redress, including for compensation for damages as a result of the unlawful processing of his/her Personal Data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.	Also, the DIFC DPL provides for judicial review and statutory appeals. Lastly, where exemptions for providing individual rights are exercised by a public authority or other Controller or Processor, they must maintain a register and justification for such exemption that the Commissioner may inspect at any time. The Commissioner may also, based on the register, make a finding of contravention or non-contravention of the DIFC DPL, and issue directions and fines accordingly.
Collection of PD for law enforcement and national security When assessing the adequacy of the level of protection in a third country, it is necessary to take into account "relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to Personal Data as well as the implementation of such legislation…". The application of such guarantees may differ in the fields of law enforcement and national security access to data. Still, these guarantees need to be respected for access to data, whether for national security purposes or for law enforcement purposes: 1) Processing should be based on clear, precise and accessible rules (legal basis) 2) Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated 3) The processing has to be subject to independent oversight 4) Effective remedies need to be available to the individuals	YES - Article 28, Article 10(1)(c), Article 11(h)

12 DIFC Commissioner's adequacy decision-making process

12.1 Foundations

12.1.1 DIFC's adequacy decision-making process is based on the EU and UK processes. DIFC have self-assessed the DIFC DPL's compatibility with international standards against the EU updated adequacy referential and the UK Explanatory Framework for Adequacy Discussions - Section D, and have actioned any necessary updates to fill apparent gaps and mitigate risks.

12.1.2 A hybrid of these processes serves as one element in the overall assessment of other jurisdictions' data protection laws and culture. As such, DIFC is deriving its own independent decisions and, in doing so, is leading other data protection supervisors to meet and potentially exceed the standards that DIFC, the UK and the EU share in common.

12.1.3 For instance, a draft decision recently submitted to the Commissioner for approval includes conditions to ensure continuous development of safeguards, monitoring, and review of onward transfers, and appends an undertaking requiring compliance with the DIFC DPL generally and Article 28 specifically. Amongst the many positive outcomes envisioned for this approach (some of which have already seen first-hand) is that other regulators and the entities they supervise will move beyond basic compliance to embrace active, dynamic development of privacy principles and priorities.

12.2 DIFC Ethical Data Management Risk Index

12.2.1 As the world has seen from the Schrems I and II decisions, the current safeguard mechanisms for international transfers are subject to recurring and very clinical scrutiny. Having the 'same law' in theory as another jurisdiction does not mean the data, upon arrival, will get in practice the 'same treatment' as at home.

12.2.2 To address this, the Commissioner's Office has devised with its own way of assessing the real risks in a jurisdiction; risks negatively impacting Data Subjects' rights, risks of breach or accidental data loss, risk of contravention of the local or any application of data protection law.

12.2.3 By creating a risk assessment tool to evaluate not only the similarities between privacy laws but also the cultural, operational and business environments in any one country or international organisation, an ethical data management risk index comes to bear.

12.2.4 On the basis of this risk assessment, much like the Transparency International Corruption Index, the "DIFC Ethical Data Management Risk Index" would be used to determine additional, enhanced due diligence and

contractual requirements an organisation should implement when processing Personal Data in the given environment.

12.2.5 In the same way as enhanced due diligence in the AML space and ensuing additional supporting documentation or undertakings necessary to mitigate risk, processing operations in countries posting a high privacy risk would also need the support of additional contractual, policy, accountability and supervisory requirements from within the organisation itself.

12.2.6 Much like a rating of a hotel or restaurant on popular crowd-sourced hospitality review sites, the risk index shows ratings on various thematic scales, such as culture of privacy, frequency of fines for data breaches or contraventions of laws, likelihood of compliance with security/privacy obligations or appointment of a DPO. Each such element will be explained when it is expanded, to demonstrate the research and decision-making process applied to its determination.

12.2.7 The intention is to change the way supervisory authorities and Controllers or Processors ensure proper, thorough implementation of data protection laws not because governments mutually agree their laws are similar, but because the Controllers and Processors that comply with them really, fully comprehend the obligations set upon them and comply.

12.2.8 The aim is also, if executed properly, to encourage better oversight and information sharing amongst privacy regulators as those very Controllers or Processors in higher risk jurisdictions may even call for compatible data protection laws and regulatory participation and influence on the operating environment in order to compete with the lower risk jurisdictions.

12.2.9 Please see further information and announcements about the EDMRI here and in Appendix D.

12.3 Main achievements

12.3.1 The DIFC Commissioner's Office is a full Member of the Global Privacy Assembly and is very active in several key working groups, including the International Enforcement Cooperation working group. It is also a Member of the Global Privacy Enforcement Network (GPEN).

12.3.2 The Commissioner has issued adequacy decisions regarding several key jurisdictions and frameworks including Singapore, South Korea, the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPRs)[85] and the California Consumer Privacy Act and Regulations. These decisions are available at this link.

[85] The Commissioner also recognized the Privacy Recognition for Processor (PRP) for Singapore entities certified under this scheme.

12.3.3 Regarding the CBPR / PRP adequacy assessments, given that they are certification schemes rather than privacy regimes implemented by a sovereign country, in accordance with the DPL, the Commissioner has approved them in accordance with Article 27(2)(e), Article 46(4) and Article 50(1).

12.3.4 The CBPR and PRP decisions apply in the context of onward transfers from entities certified under these systems in Singapore or South Korea, as relevant, to any entities anywhere in the world operating under a certification issued by an appropriately accredited body accredited within either framework.[86]

12.3.5 The Commissioner's Office is a participant in the Global Cooperation Arrangement for Privacy Enforcement (CAPE) as part of its ongoing and active relationship with the Global Cross Border Privacy Rules Forum, the international offshoot of the APEC body.[87]

12.3.6 Lastly, the DIFC has been selected as a primary partner with the UK for review and recognition of equivalence with the UK GDPR. The press release is available at this link.

[86] "Accountability Agents" are currently the accredited bodies permitted in the CBPR / PRP system to issue certifications to entities. Please see the CBPR website and CBPR program requirements for further information.

[87] Global CBPR Forum and Global CAPE

Part 6: Data flows in DIFC

13 Data processing and flows analysis

13.1 Description of data flows and controls in place

13.1.1 DIFCA has prepared a detailed analysis of data flows and systems based on both the UK ICO guidance for processing self-assessment and ISO 27001 certification requirements.

13.1.2 An extract is presented below, demonstrating the substance of DIFCA data flows and management of them:

How does DIFCA collect, use, store and delete data?	Provided information asset register and a list of sources of information, including but not limited to sources of data (direct from the Data Subject) and indirect (external sources), use cases, data sharing relationships and retention / archiving requirements.
Does DIFCA collect / share Personal Data from / with any internal stakeholders or external third parties?	See above
What categories of Personal Data are collected / shared?	Provided sample departmental Doc and Non-doc asset registers. "Docs" means any document type. "Non-Docs" mean information stored as attributes (databases, etc).
Provide a description of the controls (technical, organizational, contractual, policies / procedures, training, etc) in place to assure the security of the Personal Data.	Provided a list of relevant contractual, organisational and technical controls, as well as data governance and policy information.
What types of processing in DIFCA operations have been identified as likely to be high risk?	Assessed the above in the context of the definition of High Risk Processing activities as set out in DIFC DPL. Please HRP assessment tool for further information.

13.1.3 The detailed assessment is similar to the one that DIFC registered entities would experience and demonstrates the Commissioner's expectations when reviewing entities from a supervisory perspective.

13.1.4 Further detailed information is available upon request.

Appendix A: Promulgation of Federal Legislation

1 Federal Laws

1.1 The UAE Constitution outlines the following process for promulgation of federal laws:

(a) *preparation of a bill by the Council of Ministers[88] and submission to the Federal National Council (**FNC**);[89]*

(b) *submission of the bill to the President[90] for his approval and presentation to the Supreme Council[91] for ratification;*

(c) *signature of the bill by the President after ratification by the Supreme Council.*

1.2 If the FNC inserts an amendment that is not acceptable to the President or the Supreme Council, or if the FNC rejects the bill, the President or Supreme Council shall refer it back to the FNC for a second time. If the FNC introduces an amendment upon second submission that is not acceptable to the President or the Supreme Council, or if the FNC rejects the bill, the President may nonetheless promulgate the law after Supreme Council's ratification.

1.3 If a situation requires the promulgation of federal laws when the FNC is not in session, the Council of Ministers may issue them via the Supreme Council and President provided that that FNC is notified at its next meeting.

2 Decree Laws

2.1 If there is a need for urgent promulgation of federal legislation between sessions of the Supreme Council, the President and Council of Ministers may promulgate the necessary laws in the form of decrees which have the force of law provided they are not inconsistent with the Constitution.

2.2 Decree-laws must be referred to the Supreme Council within a week for assent or rejection. If not approved, they cease to have force of law.

3 Ordinary Decrees

3.1 While the Supreme Council is out of session, it may authorise the President and Council of Ministers collectively to promulgate decrees that may be ratified within the power of the Supreme Council. This does not include ratification of international agreements and treaties or declarations of war.

---

[88] The Council of Ministers (or Cabinet) is the executive branch of the federation and consists of the Prime Minister, Deputy Prime Minister and the Ministers of the UAE (Foreign Affairs; Interior; Defence; Finance, Economy & Industry; Justice; Education; Public Health; Public Works & Agriculture; Communications, Post, Telegraph & Telephones; Labour & Social Affairs; Information; and Planning). See further: https://u.ae/en/about-the-uae/the-uae-government/the-uae-cabinet

[89] The consultative council and parliamentary body of the UAE. The FNC is composed of 40 members (part-elected, part-appointed) with between four and eight seats distributed to each of the member Emirates. See further: https://u.ae/en/about-the-uae/the-uae-government/the-federal-national-council-

[90] Elected by the Supreme Council from among its members. See further: https://u.ae/en/about-the-uae/the-uae-government/the-president-and-his-deputy

[91] The highest constitutional authority in the UAE and consisting of the Rulers of all Emirates in the Federation, each with a single vote. See further: https://u.ae/en/about-the-uae/the-uae-government/the-federal-supreme-council

Appendix B: UAE Smart Data Framework (SDF)

The UAE Smart Data Framework (SDF) demonstrates the importance the UAE government places on privacy, data protection and individual rights. Until the national privacy law is enforceable, the SDF is one of many ways the UAE government implements safeguards and holds importers, including government authorities, accountable for responsible processing and transfer of Personal Data with trust. The SDF is broken down into **Principles and Standards (Part 1)** and **Implementation Guide (Part 2**), among other relevant documents.

Part 1: SDF Data Exchange (DE) Standards

The Data Exchange Standard dedicates a full area of specifications (Area C) to data protection, privacy, access rights, and permissions to ensure that access to data is appropriate, conformant, and protects individual privacy. Before detailing such specifications, it is important to explain how classification of data to different categories as per the framework provides safeguards to Data Subjects.

Categories and Criteria for processing data by government authorities

The classification of each category of data is the first level of safeguards taken into account and applies limitations with respect to how and for what purpose such data may be used. The table below sets out criteria for assessing what data falls into each class, with examples. Deciding the classification level (i.e., Open, Confidential, Sensitive and Secret) depends on a risk assessment that the government entity must apply to assess the level of damage that may result from unrestricted disclosure of the data to government authorities. When reviewing the table below, please note the alignment of data types with the definitions found in the DIFC PDL and similar laws including the UK GDPR and the EU GDPR. The safeguards and limitations that the classifications under the Data Exchange Standard afford are as follows:

Category of Data / Personal Data	**Criteria**
Open	**Criteria**: Data that can be openly disclosed to individuals, governmental, semi-government entities and private sector for use, re-use and sharing with third parties. This should be the default classification for all non-Personal Data, and exceptions to this should have a documented rationale that clearly explains why open publication of the data would contravene specific criteria listed below that require classification as Confidential, Sensitive or Secret.

Category of Data / Personal Data	Criteria
Confidential	**Criteria**: This is the default classification for datasets containing Personal Data which is non-sensitive. "Personal Data" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Non-sensitive Personal Data refers to all types of personal information which are not 'confidential' (as defined in the criteria for Sensitive Data below). In addition, data should be classified as Confidential if unrestricted disclosure or exchange of the data cause No damage to government bodies, companies or individuals such as: • Adversely affecting or preventing the ability of a Government Entity to carry out its day to day duties • No damage to assets, or limited financial loss of an Entity, company or individual • Limiting the competitiveness of companies and negatively affecting the principle of equal opportunities • Adversely affecting public safely, criminal justice and enforcement activities.
Sensitive	**Criteria**: This is the default classification for datasets containing sensitive Personal Data. Sensitive Personal Data are Personal Data that directly or indirectly reveal an Individual's family, racial or ethnic origin, sectarian origin, political opinions, religious or philosophical beliefs, their union membership, criminal record, health, sexual orientation, genetic data or biometric data In addition, data should be classified as Sensitive if unrestricted disclosure or exchange of the data may cause limited damage to government bodies, companies or individuals such as: • Infringing Intellectual Property Rights • A significant decline in the ability of one of the bodies to carry out its functions, limited damage to its assets, or significant financial loss • Causing limited damage to companies that could lead to loss of competitiveness, or loss of some of its core cognitive and intellectual advantages or incurring heavy financial loss • Limited damage to the operational effectiveness of the police, security forces, military forces, intelligence services or the administration of justice • Limited damage to relations with friendly governments or damages to international relations resulting in formal protest or sanctions.

Category of Data / Personal Data	Criteria
Secret	**Criteria:** Data the unrestricted disclosure or exchange of which may cause significant damage to the supreme interests of the United Arab Emirates and very high damage to government bodies, companies or individuals, such as: • Disclosing any personal information of a VIP (very important person) or infringing any Intellectual Property Rights of a VIP • A significant or noticeable negative impact to the supreme interests of the United Arab Emirates • A sharp decrease in the ability of one of the vital bodies to carry out its functions, or very high damage to its assets, heavy financial loss, clear negative impact on the image of the body and a loss of public confidence in such body and in the government in general • Causing significant damage to private sector entity that have vital and strategic roles in the national economy, which may lead to heavy financial losses, bankruptcy or loss of its leading role • Seriously endangering the safety and lives of certain individuals associated with a security role (e.g., security forces and police) or as parties to serious judicial cases (e.g., witnesses) • Information the disclosure of which would negatively affect the maintenance of security and the administration of justice, or cause major, long-term impairment to the ability to investigate or prosecute serious crimes.

From Section 3.4 on Data Exchange Standards (from Part 1 of the Standard)

Once classification is applied to data categories, the relevant standards are enumerated. The most relevant standards that incorporate essential safeguards and limitations to processing data in the above categories are the Data Protection and Privacy Standard [DE6] and the Shared data access permissions standard [DE7]. They have been copied from the Data Exchange Standards document and are set out below, with emphasis added where the safeguards and limitations provided align with those in DIFC law and regulations.

Data protection and privacy standard [DE6]

DE6	Data protection and privacy	
Specification type	☐ Dataset Processing Specification	☑ Data Management Specification
Purpose	The purpose of this Specification is to: • ***Ensure that people and businesses in the UAE have trust and confidence that their data is ethically used and enjoys strong levels of protection and privacy*** • Build a culture of privacy awareness and responsibility within officials dealing with data • Ensure Personal Data management and infrastructure is resilient and secure • Ensure data is only used in ways that meet documented ethical standards • Enable uniformity and consistency in decision making in relation to data protection and privacy.	
When to use	Across all stages of the data management lifecycle: creating, processing, analysing, storing, exchanging and re-using data.	
Responsibility	The Director of Data [92]has responsiblity for ensuring that the Entity has the systems, infrastucture and controls necessary to comply with this Standard specification, and that these operate effectively and consistently. The Data Custodian within the Entity who is accountable for a specific dataset is responsible for ensuring that the requirements of this specification are met in relation to that dataset.	
Requirements		
Mandatory	DE6.1	All Entities should work towards achieving, across all personal and commercial datasets for which they are responsible, full compliance with the Data Privacy Principles set out in this specification[93]: 1. Consent 2. Transparency 3. Purpose 4. Proportionality 5. Personal access and control 6. Security 7. Sectoral compliance 8. Documentation 9. Awareness 10. Accountability
	DE6.2	***Government Entities should publish these Data Privacy Principles on their websites, and provide complaints and redress mechanisms for Data Subjects who believe they are failing to manage their data in accordance with the above principles. (i.e., notice)***

[92] *Please see the full Standards documents for definitions and further information.*

[93] *The principles listed here demonstrate that (i) processing by UAE entities should be based on clear, precise and accessible rules (legal basis); (ii) necessity and proportionality with regards to legitimate objectives pursued; and (iii) rights and redress mechanisms available to all Data Subjects.*

DE6	Data protection and privacy	
	DE6.3	Government Entities should assess where there are gaps in how their current data management practices conform with these Data Privacy Principles, develop plans to close these, and share these plans with the Federal Data Management Office.
Recommended	DE6.4	Semi-government and Private Sector Entities are also recommended to embed the UAE Privacy Principles within their own data management practices in order to build a cohesive national system of trusted data exchange within a strong framework of data protection and privacy.
Standard Inter-dependencies	• **[DC1] Data Classification** sets out the criteria that Entities should apply when determining whether a dataset contains Personal Information or Commercial Information of the sort that is covered by the privacy requirements of this specification. • The access rights that should be attached to a dataset after application of the principles in this Standard should be documented through either **[DE5] Open Data License** or **[DE7] Shared Data Access Permissions**, and through **[DE2] Metadata**.	
References to Implementation Guide	**Guidance Note 5.3** provides a more detailed description of the principles in this Standard, together with advice on a best practice process to follow when applying these to an individual dataset.	
Version History	V1.0	

Shared data access permissions standard [DE7]

DE7	Shared data access permissions	
Specification type	☐ Dataset Processing Specification	☑ Data Management Specification
Purpose	***This Specification describes principles and practices for permitting access to Confidential and Sensitive Data, in a way that facilitates cross-government service integration and complies with the principles of [DE6] Data protection and privacy.***	
When to use	When preparing *Confidential or Sensitive* data for exchange with another Entity for the first time, Entities should document who is permitted to have what level of access to the data in compliance with this Specification. Entities should then apply this Specification when responding to future requests for additional access permissions.	
Responsibility	The Director of Data has responsiblity for ensuring that the Entity has the systems, infrastucture and controls necessary to comply with this specification, and that these operate effectively and consistently. The Data Custodian within the Entity who is accountable for a specific dataset is responsible for ensuring that the requirements of this specification are met in relation to that dataset.	
Requirements		
Mandatory	DE7.1	Government Entities should follow the five **Access Permission Principles** described in this specification whenever they share their *Confidential or Sensitive* data with a third party:

DE7	Shared data access permissions	
		1. Entities should facilitate cross-government sharing of their data 2. ***Data sharing should protect personal and commercial privacy*** 3. Use of the Smart Data Electronic Platform 4. ***Data Sharing Access Permissions should be documented*** 5. Access to shared data should be secured and audited
	DE7.2	***Government Entities should assess where there are gaps in how their current data management practices conform with these UAE Access Permissions Principles, develop plans to close these, and share these plans with the Federal Data Management Office.***
	DE7.3	Government Entities should respond promptly in writing to requests for data sharing from other Entities, and notify the Federal Data Management Office of all such requests.
Recommended	DE7.4	***Entities are also recommended to make the audit functionality that is required under Access Permission Principle [6] openly available for use by individual Data Subjects.***
Standard Inter-dependencies	• **[DC1] Data Classification** sets out the criteria that Entities should apply when determining whether a dataset should be classified as *Confidential or Sensitive*, and is thus subject to this specification. • The access rights that are set out in the Shared Data Access Permissions required by this standard should comply with the requirements of **[DE6] Data protection and privacy**.	
References to Implementation Guide	**Guidance Note 5.3** provides advice on a best practice process to follow when a) documenting an initial set of Shared Access Data Permissions for a dataset and b) responding to requests from other Entities for additional Shared Data Access Permissions .	
Version History	V1.0	

Part 2: Implementation / Data Conformance Process

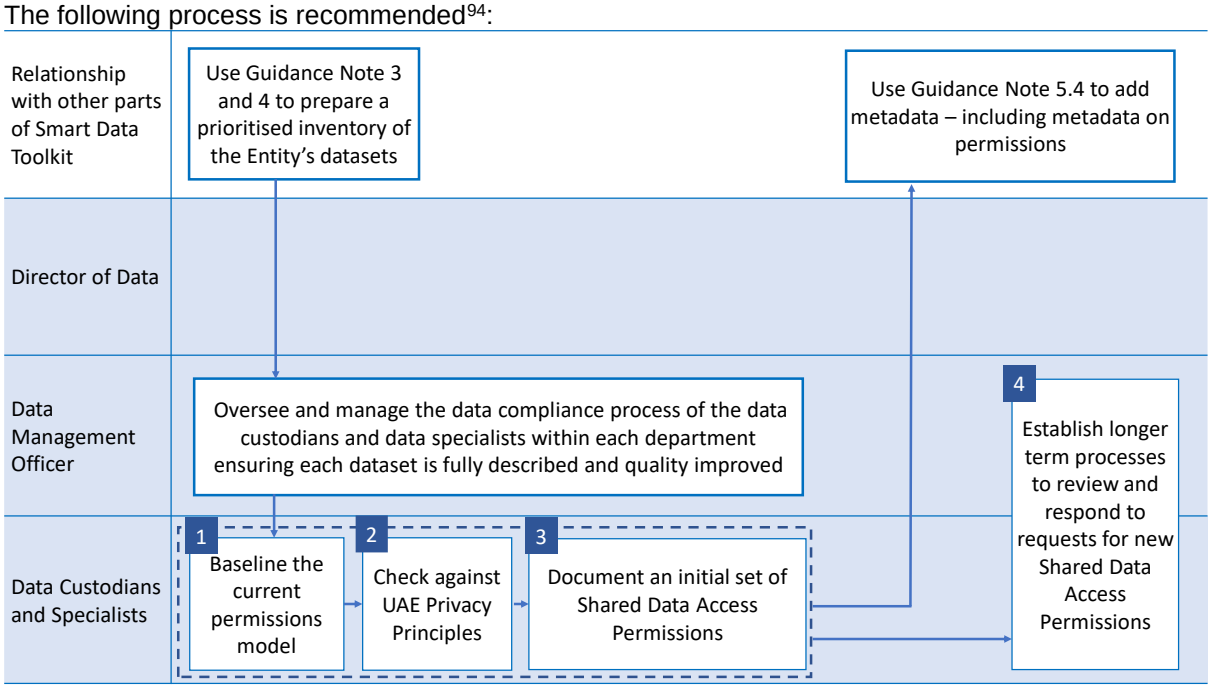
This section describes the protocols in place to ensure proper government body data exchange, that sharing is in line with the appropriate classification levels set out about and that access is limited by query / response type (i.e., yes or no regarding an age search rather than providing date of birth).

5.3 Documenting a permissions model for shared data

Purpose	This Guidance Note outlines the recommended process for determining who may access a dataset and with what level of access in conformance with the **[DE7] Shared data access permissions** specification.
When to use	When preparing Confidential or Sensitive data for exchange with another Entity for the first time. Also when responding to future requests for additional access permissions.

Responsibility	Data Custodian.

Process
For each dataset in the current prioritized batch being catalogued, the responsible Data Custodians need to ensure that the requirements of the **[DE7] Shared data access permissions** specification are met in respect of Confidential and Sensitive Data.
The following process is recommended[94]:



1. Baseline the current permissions model

Your dataset will already have a set of permissions associated with it, even if this is simply current practice rather than a documented policy. So the starting point is to document the baseline position around who is permitted to access the data.

2. Check against UAE Privacy Principles

The **[DE6] Data protection and privacy** specification sets out a set of UAE Privacy Principles which all Government Entities should seek to apply when managing data that contains Personal Data or commercial data. Having documented current practices around granting access permissions to data, you should check that those practices are compliant with these Privacy Principles. Particular issues to consider are:

- Does the Entity have the consent of the Data Subject to share their data with all those people who currently access it?
- If not, is the dataset covered by sector specific regulations which mean that such consent is not required?
- Are there controls in place to ensure that people permitted access to the data may only use it for specified business purposes?
- Is the level of access proportionate to the stated purpose? (For example, if an official has a business need to check whether an individual is over 18, they should be permitted yes/no query access to the data rather than being able to see the date of birth of the individual.)

[94] *Steps 1 to 3 are detailed below this table; step 4 is self-explanatory.*

Entities should embed the following UAE Data Privacy Principles in their data management practices, and in those of third parties contracted to manage data and services on their behalf.[95]

Data Privacy Principles		Description
1.	**Consent**	• Personal Data in relation to individuals and Commercial Data in relation to Private Entities should not be disclosed or shared without the Data Subject's consent. • When providing a service to an individual or a Private Entity, Government Entities should seek the consent of that Data Subject for the data to be exchanged with other Government Entities for the purpose of enabling any Government Entity to provide services to the Data Subject without the need for the Data Subject to provide the same information again.
2.	**Transparency**	• Data subjects should be informed - at the point of data collection - when and by whom their data is being collected, why it is needed, and how it will be used.
3.	***Purpose***	• *Data should only be used for limited and explicitly stated purposes and not for any other purposes without first gaining informed consent from the Data Subject.*
4	***Proportionality***	• *When data is requested and stored, the type of data collected should be the minimum required to carry out the stated purpose, individual users of the data should only be given the minimum access to that data that they need, and the data should not be kept for longer than is necessary for that purpose.*
5	***Personal access and control***	• *Data subjects should be enabled to:* – *Access and take copies of data that is held about them* – *Correct inaccuracies in data that is held about them* – *Request removal of data that is held about them, but is no longer relevant or applicable to the business of the Entity*
6.	**Security**	• Collected data should be protected by robust and tested security safeguards (technical and organizational) against such risks as loss and unauthorized access, destruction, use, modification or disclosure.
7.	***Sectoral compliance***	• Each sector has its own laws and regulations, some of which relevant to the basis on which data can be shared with other entities or with public. Examples of these laws include the United Arab Emirates Penal Code, the Copyrights' Act, and the Telecommunications' Act. • *Entities should ensure they comply with both relevant sectoral regulations and this Standard, and should notify the Federal Data Management Office in the event of any perceived conflict.*
8.	**Documentation**	• Entities should document who is permitted to access each data set, either in the form of the **[DE5] Open Data License** (for all Open Data) or through a documented set of **[DE7] Shared Data Access Permissions**. • Entities should produce and maintain privacy metadata in relation to these access permissions, as part of their broader work on **[DE2] Metadata**, and store this in their Data Inventory.
9.	**Awareness**	• Entities should develop an awareness programme for their data privacy policy, which shall be disseminated to all staff within the Entity who manage data (both from business and technical areas) in order to remind them of the Entity's obligations and their personal responsibilities concerning data privacy.
10	***Accountability***	• *Entities should establish and publicise effective complaints and redress mechanisms for Data Subjects who believe they are failing to manage their data in accordance with the above principles.*

[95] *The contents of this table have been condensed. The full table is available in Part 2 of the Standards set of documents.*

3. Document an initial set of Shared Data Access Permissions

Develop a documented set of initial Shared Data Access Permissions. Normally, this will simply codify the existing data sharing practices that are in place for the dataset - perhaps modified following the privacy conformance assessment at Step 2. These Shared Data Access Permissions should cover:

- **Who may have access to the shared data**.
- **What purpose this access is for**. This documentation is particularly important to ensure conformance with the 'purpose' and 'proportionality' principles of **[DE6] Data protection and privacy** and to enable effective auditing.
- **The level of access that they may have**.

Mandatory actions

In applying these principles, each Government Enterprise should:

- **Develop a detailed Data Sharing Plan, setting out how they will implement the Data Exchange Principles** described in this Standard**,** including any investments in systems and processes that they will need. They should share this Plan with the Federal Data Management Office.
- **Respond in writing within a reasonable time** to requests for data sharing from other Entities

Recommended actions

When implementing Access Permission Principle 5 ("Access to shared data should be secured and audited"), Government Entities are recommended to ***make this audit functionality openly available for use by individual Data Subjects***. This means:

- Configuring electronic platforms and supporting business processes so that individual Data Subjects (citizens, residents and businesses) can see an audit trail of who accessed their data, and for which documented purpose (excluding security service or law enforcement access)
- ***Providing mechanisms by which Data Subjects can raise concerns / escalate if they believe access has been misused.***

Appendix C: DIFC Government Data Sharing Policy

Template for general government data sharing policies that may be used by DIFC entities or their affiliates, third party vendors, etc.

Sample Government Data Sharing Policy

Appendix D: Template – Article 28 Government Data Sharing MOU

Sample A28 MOU Template

Appendix E: EDMRI and EDMRI+

EDMRI and EDMRI+