OVERVIEW OF DIFC DATA PROTECTION LAW AND REGULATIONS

Commissioner of Data Protection

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 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, including enactment of regulations to address processing of personal data in autonomous and semi-autonomous systems (DIFC DP Regulation 10).

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

---

[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

> "*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.

1 Authority of the DIFC

1.1 Powers derived from UAE Federal Authority

1.1.1 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*"*[8] *pursuant to the Financial Free Zone Law and its Implementing Regulation.*

1.1.2 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.

1.2 Powers derived from Dubai Emirate Authority

1.2.1 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)**[9] 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"*;*[10]

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

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

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

[8] Article 1, DIFC Law
[9] Law No. 5 of 2021 Concerning DIFC
[10] Article 3(a)(1), DIFC Dubai Law

(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.

1.2.2 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*".[11]

1.2.3 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*."[12]

1.2.4 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.[13]

1.2.5 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 1.2.3 above).

1.2.6 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 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

[11] Article 9(b)(3), DIFC Dubai Law
[12] Article 22(b), DIFC Dubai Law
[13] Article 8(a), DIFC Dubai Law

in the DIFC, which outlines a "waterfall" of applicable laws beginning with DIFC law and ultimately concluding with the law of England and Wales.[14] This interpretation has been followed in DIFC case law.[15]

1.3 Data protection in the DIFC

1.3.1 In light of:

(a) *the exemption of application of Federal civil and commercial laws under the Financial Free Zone Law (see paragraph 1.1.1 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 1.1.1 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 1.2.1 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 1.2.2 to 0 above),*

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

1.3.2 The Data Protection Law 2007 (DIFC Law No.1 of 2007)[17] 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.

1.3.3 The current law, the Data Protection Law, DIFC Law No. 5 of 2020 (the "DPL" or "DIFC DPL")[18] 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

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

[15] 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)

[16] DIFC Data Protection Law 2004

[17] DIFC Data Protection Law 2007

[18] DIFC Data Protection Law 2020

same date.[19] The DPL was amended and an updated version published in March 2022.[20]

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

1.3.5 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.

1.4 DIFC Commissioner of Data Protection

1.4.1 The DIFC DPL grants the President of the DIFC the power to appoint a person to administer the Law (the Commissioner).[21] 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.

1.4.2 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*

(c) *to promote greater awareness and public understanding of data protection and the requirements of the DIFC DPL and the Regulations in the DIFC.*[22]

1.4.3 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

[19] DIFC DPL 2020
[20] DIFC DP Regulations
[21] Article 43(1), DIFC DPL
[22] Article 46(2), DIFC DPL

as preparing draft regulations, standards/codes of practice or guidance for approval of the DIFCA Board of Directors.[23]

1.4.4 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.

2 Legal Framework – DIFC Data Protection Law and Regulations

2.1 Internationally recognized data protection principles and guidelines

2.1.1 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 Privacy Guidelines or Council of Europe Convention 108+, internationally recognized data protection laws such as the GDPR and UK GDPR, and the laws of Colombia. Please see below for details.

2.2 Compatibility of the DIFC DPL principles with similar laws

2.2.1 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

[23] Article 46(3), DIFC DPL

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***
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
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

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***
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

3 Rights of Data Subjects

3.1 Comparable Data Subjects' rights and protections

3.1.1 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.

3.2 Guidance and assessment tools

3.2.1 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.

4 Legal Duties of Controllers and Processors

4.1 Accountability and compliance requirements

4.1.1 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.

4.1.2 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. All such obligations are again as per the GDPR and the UK GDPR, and further guidance can be found as follows:

4.2 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/

4.3 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

5 Overview of Government information requests in the UAE

5.1 Establishment and powers of UAE government authorities

5.1.1 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*".[24]

5.1.2 Federal ministries are also required to practice their powers in line with the guidelines of the Cabinet and the federal laws.[25] 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.[26] 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.

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

5.2 Government data sharing in the DIFC

5.2.1 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**).[27] 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.[28] The DIFC DPL obliges Controllers to undertake similar assessments of governmental data requests.

5.2.2 To fully implement the DIFC Government Data Sharing Policy, DIFCA has executed Memoranda of Understanding (**MOU**) for data sharing with at least

[24] Article 1, Federal Law No. 1 of 1972
[25] Article 20, Federal Law No. 1 of 1972
[26] Article 5, NMC Law
[27] Tools and Templates
[28] Amazon article

two (2) UAE authorities from which it typically receives the majority of data requests, with others in train. The template MOU[29] 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.

5.2.3 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.

5.3 Government requests to DIFC Controllers and Processors

5.3.1 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.

5.3.2 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.

5.3.3 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.

5.3.4 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 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.

5.3.5 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

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

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.

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

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

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

6.1.1 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.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.2 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 Financing of Illegal Organisations	- Law No. (26) of 2015 regulating Data Dissemination and Exchange in the Emirate of Dubai ("Dubai Data Law") .
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.	- 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") .

7 Limitations and Safeguards

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

7.1.1 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.

7.1.2 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.[30]

7.1.3 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:

(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")[31] 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.

7.2 In UAE regulations

7.2.1 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.

7.2.2 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".

7.2.3 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 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."

7.2.4 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."

7.3 In local (Emirate) laws and frameworks

7.3.1 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.

7.3.2 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."

7.3.3 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".

i. 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."

ii. 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.

iii. 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.

[30] DIFC Data Protection Guidance webpage

8 Safeguards between DIFC and UAE Public Authorities

8.1 Engagements with non-DIFC authorities

8.1.1 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)[32] 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.

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

8.2 Requests from non-DIFC bodies

Training and culture of DIFCA staff

8.2.1 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

8.2.2 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.

8.2.3 Any queries are discussed with the relevant authority.

a) 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.

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

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

[32] 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.

8.3 MOUs and other binding agreements

Updating existing MOUs and agreements

8.3.1 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.

8.3.2 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

8.3.3 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.

9 DIFC Commissioner of Data Protection

9.1 Independent, competent public authority

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

9.2 Commissioner's powers and functions

9.2.1 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 ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any	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. Also, the DIFC DPL provides for judicial review and statutory appeals. Lastly, where exemptions for

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.	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)

10 DIFC Commissioner's adequacy decision-making process

10.1 Foundations

10.1.1 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.

10.1.2 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.

10.1.3 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.

10.2 DIFC Ethical Data Management Risk Index

10.2.1 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.

10.2.2 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.

10.2.3 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.

10.2.4 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.

10.2.5 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.

10.2.6 Muh 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.

10.2.7 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.

10.2.8 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.

10.2.9 Please see further information and announcements about the EDMRI here and in Appendix A.

10.3 Main achievements

10.3.1 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).

10.3.2 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)[33] and the California Consumer Privacy Act and Regulations. These decisions are available at this link.

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

10.3.3 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).

10.3.4 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.[34]

10.3.5 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.[35]

10.3.6 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.

[34] "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.

[35] Global CBPR Forum and Global CAPE

11 Data processing and flows analysis

11.1 Description of data flows and controls in place

11.1.1 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.

11.1.2 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.

11.1.3 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.

11.1.4 Further detailed information is available upon request.

Appendix A: EDMRI and EDMRI+

EDMRI and EDMRI+