DIFC

ARTICLE 28: PUBLIC AUTHORITY ACCESS TO PERSONAL DATA & INDIVIDUALS' REDRESS OPTIONS

Commissioner of Data Protection

DIFC

CONTENTS

1. Introduction

Part 4 of the Data Protection Law, DIFC Law No. 5 of 2020 (the "DP Law 2020") and Section 5 of the Data Protection Regulations 2020 (the "Regulations") cover the topic of Data Export and Sharing, which deals with transfers of Personal Data outside of the DIFC. In that context, Article 28 of DP Law 2020 prescribes the process of assessing requests from public authorities with respect to the disclosure and transfer of Personal Data. DIFC's Article 28 Guidance (the "Article 28 Guidance") will address the circumstances and methods for safe, controlled data sharing when approaching such government demands.

Personal Data is defined in the DP Law 2020 as, "Any Data referring to an Identifiable Natural Person" and Special Category Data is defined as, "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person." Such data includes but is not limited to name, address, business or personal email address, business or personal phone numbers, geolocations, job title or other employee data, health and biometric data, religious affiliations or criminal history.

Personal Data generally can be any information that when viewed together (or in some cases is so unique) it clearly identifies a living individual. It could be data about clients, employees, suppliers, or family members, to name a few categories of Personal Data. Many, if not all, organisations process Personal Data.

Public authorities of any country may, for various reasons, submit requests to your organisation that will result in disclosure, sometimes for sensitive purposes, and transfer of Personal Data out of the DIFC. When faced with such requests, you will need to adequately apply the safeguards that Article 28 of DP Law provides. This guidance will help navigate responses to these government enquiries.

The defined terms used herein have the same meaning as the defined terms in the DP Law.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the DIFC Commissioner of Data Protection (the **Commissioner**) either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

2. Scope

Although the DIFC has historically relied on UK and EU data protection and privacy principles as a guiding tool for developing its own data protection framework, the incorporation of Article 28 into the DP Law is a novel approach undertaken by the DIFC, in order to address the issue of public authorities accessing personal data pursuant to transfer requests.

Generally, due to DIFC's historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by UK authorities, from a common law perspective, this guidance should be read in conjunction with those existing UK and EU laws and guidance on the same topic, with which the DP Law is also aligned.

Please note that ***this guidance expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice****. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.*

3. Article 28 Obligations

Article 28 of the DIFC DP Law 2020 sets out specific obligations regarding **sharing Personal Data with importing government / public authorities or law enforcement** to ensure data shared with them is controlled in some manner. Within this context, DIFC's approach in this Article was formulated in light of the judgement issued by the Court of Justice of the European Union in the Schrems II case (C-311/18), as a means to tackle the challenges encountered by DIFC exporting entities when faced with government requests of this nature.

While these authorities have powers prescribed to them by applicable national or regional laws, there are protections set out in the DP Law 2020 in relation to the sharing of Personal Data by DIFC Controllers or Processors with them under Article 28.

Article 28 provides the exporting entity with a **structured approach in navigating responses to requests** from government authorities, with the aim of documenting the decision properly, demonstrating that the issues of government access and subsequent processing practices have been considered and safeguarded.

Article 28 prescribes the process as follows, consisting of two phases:

i. **Phase 1**, under Article 28(1), which provides for the initial assessments you ought to make when receiving the request; and

ii. **Phase 2**, under Article 28(2), which provides for the baseline considerations you must make before transferring (or not) the data to the public authority.

Furthermore, under Article 28(3) you also have the option to consult with the Commissioner's Office in relation to such a government request, as will be explained later.

Finally, remember that in any case, where Personal Data is leaving the DIFC to a jurisdiction that is either not deemed by the Commissioner to have an equivalent data protection law to that of DIFC DP Law 2020, and / or where certain risks in relation to the importing entity are higher than usual, as set out in the Ethical Data Management Risk Index, you will be required not only to apply additional safeguards such as the DIFC Standard Contractual Clauses, or conduct additional due diligence to mitigate the risk and document your decision-making, or both. All supporting information for these obligations are outlined on the Data Export & Sharing sub-menu of the DIFC DP website.

Phase 1: Initial process to be followed when receiving the request

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 undertake the following actions:

Step 1: Determine the validity and scope of request

Article 28(1)(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;* […]

The first step, when receiving a request from a public authority, is to determine the validity and proportionality of the request. In that respect, your organisation needs to ensure that the request:

i. has a valid legal basis (i.e. a legally valid warrant, court order, or other specific judicial or regulatory mandate, amongst others);

ii. comes from a public entity that has the authority to make such request;

iii. is not overly broad or vague, as to cover every possible information over the Data Subjects, without rationale; and

iv. is properly served, as per the applicable law.

In addition, during this step you need to ensure that any disclosure of Personal Data is carried out solely for the purpose of meeting the objectives identified in the request from the public authority. More specifically, even though a request can have a valid legal basis, the authority could ask for more information than required to fulfil its aim. Thus, where possible, you should validate the purpose and limit the scope in order to minimize the sharing and specify the reason for the processing.

Step 2: Risk assessment and measures to minimise risks

Article 28(1)(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;* […]

The second step is conducting a risk assessment with a view to identifying potential risks to the rights of the affected Data Subjects. In other words, documenting an **impact assessment** of sharing the data versus not sharing it, taking into account the effect on the rights of the Data Subject versus the common good.

Following the completion of this assessment, you have to consider the potential **measures** you can implement to minimise the identified risks. These can include measures which relate to:

i. the Personal Data itself, i.e. redacting or minimising the data transferred by narrowly interpreting any requests to transfer only the minimum necessary data needed to comply; and/or

ii. the method of transfer, i.e. confirming the recipient / requestor is employing privacy enhancing technology, training, policies and other measures to assure the safety of the data and is utilising the appropriate technical measures to safeguard the transfer.

Step 3: Obtaining "written assurances" from the public authority (where reasonably practicable)

Article 28(1)(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;* […]

As a final step when processing the initial request, you should, where reasonably practicable, obtain appropriate written and binding assurances from the public authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 of the DIFC DP Law 2020.

Article 28(1) suggests that an exporting entity "should" take such steps, recognizing that it is not always: a) possible under applicable laws and regulations – particularly regarding prevention and investigation of alleged financial crime – or b) necessary, with respect to very basic, low risk requests, to obtain written assurances. In any case, where the importing government authority engages in the bilateral effort to agree that DP Law-based terms for sharing Personal Data with it, they both have a documented, fair opportunity to give input into the necessary safeguards and limitations, if any, on the scope of the request.

"***Reasonably practicable***" in this context broadly means an assessment of where there is room and scope to discuss safeguards and applicability of the DP Law 2020 to the transfer. Even though the DP Law 2020 will always apply, there are terms within the DP Law 2020 that permit sharing for regulatory purposes, (substantial) public interest and to prevent financial crime, amongst others. Short of the importing government authority having a court order, warrant, or other specific judicial or regulatory mandate, it will usually be "reasonably practicable" to at least have the discussion about obtaining such written assurances.

"**Written assurances**" could come in many forms. They can include:

- ✓ a basic data sharing Memorandum of Understanding (MOU);
- ✓ an annex to the DIFC Standard Contractual Clauses (SCCs);

- ✓ a simple email agreement citing Article 28 of the DP Law 2020; or
- ✓ a full data protection agreement.

You may also agree that when the purpose is fulfilled the data is returned or destroyed by the requesting authority.

The DIFC Commissioner's Office is available to consult on possible forms of "written assurances" and whether pursuit of obtaining this safeguard is warranted. An Article 28 MOU template is available on the templates section of the Accountability & Rights page of the DIFC DP website to help you get started in any case.

Phase 2: Responding to the request - baseline considerations

Following the initial assessments under Phase 1, the final decision related to whether the Personal Data ought to be transferred to the public authority must be made in accordance with some baseline considerations. The similarity here with Article 28(1)(c) is that the written assurances are documented, but the outcome of actions taken to satisfy Article 28(2) may come in the form of a DPIA for example or perhaps even a policy document to clarify to the organisation the appropriate steps for sharing data with government authorities.

According to Article 28(2), Controllers and Processors (upon reasonable notice to the controller) may disclose or transfer Personal Data to the public authority provided they have taken reasonable steps to ensure that:

a. the request from the public authority is valid and proportionate; and
b. the public authority will respect the rights of Data Subjects when processing any Personal Data shared with it by the Controller.

Step 1: Final deliberation on the validity and proportionality of the request

> Article 28(2)(a) […] *a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate;* […]

This step relates to the confirmation of the assessment you have already conducted under the 1st Phase with respect to the legal validity and proportionality of the request. Legal validity of the request is of paramount importance and a necessary requirement that needs to be fulfilled before you move forward with considering the next steps.

In light of the above, even if the public authority is invoking a valid legal basis for the request, you may want to confirm that they possess the necessary documentation, as well as forward to your organisation valid copies of such (i.e., warrant, court order, internal decision based on statutory power) to keep for your records.

Step 2: Assessing public authority's adherence to respecting the rights of the Data Subject

> Article 28(2)(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).* […]

Following confirmation that the request is legally valid and within the powers of the requesting authority, the final step is to take reasonable steps to satisfy yourself that the authority will respect the rights of the relevant Data Subjects.

Such reasonable steps include actions that you should have already conducted under Article 28(1)(b) and Article 28(1)(c), i.e.:

i. carrying out a risk/impact assessment to identify potential risks to the rights of the affected Data Subjects;
ii. employing measures to minimise such risks;
iii. confirming that the requesting authority has the appropriate privacy enhancing technology, policies and other measures in place to assure the safety of the data transferred; and
iv. obtaining "written assurances" from the public authority (where reasonably practicable).

Further to the above, to ensure proper due diligence, you should include in your consideration the following when making the transfer decision:

i. whether the jurisdiction is included in the List of international jurisdictions approved by Commissioner of Data Protection on transferring personal data;
ii. the level of risk in exporting to that jurisdiction, as identified in the DIFC's Ethical Data Management Index; and
iii. conducting and documenting your own assessment of the importing public authority based on the Ethical Data Management Risk Index (EDMRI)+ Assessment of Importing Entities, which gives the Commissioner's view of potential for risks in an importing entity's compliance environment.

The aforementioned steps **should not be approached as merely box-ticking exercises**, but rather as tools that enable you to attain a holistic view on the risk of transferring the Personal Data.

Conducting and documenting these assessments will be a strong indicator that your organisation has "*taken reasonable steps*" to satisfy the requirements of Article 28.

Article 28(3): Consultation with the Commissioner's Office

A fallback position, to consult with the Commissioner, is set out in Article 28(3). A further nuance here is that, where requested, it is possible not only that the requesting government entity and / or the consulting entity may receive guidance from the Commissioner's Office, but also that any of the entities involved may submit a complaint, seek a decision of contravention or no contravention of the DP Law 2020, seek a direction, or rely on other remedies as set out in Part 9 of the DP Law 2020, in the case of unlawful processing or other potential breaches of the DP Law 2020 that arise from the requested processing.

4. Individuals' Rights to Redress for Breach

A. Redress generally – Parts 8, 9 and 10 of the DIFC DP Law 2020

The Commissioner's objectives, which generally open the gateway for redress remedies to be sought, are defined under Article 46(2) of the DP Law 2020 as follows:

(a) to monitor, ensure and enforce compliance of the DP Law 2020;
(b) to promote good practices and observance of the requirements of the DP Law 2020 and the Regulations by a Controller or Processor; and
(c) to promote greater awareness and public understanding of data protection and the requirements of the DP Law 2020 and the Regulations in the DIFC.

The Commissioner has a range of powers available under the DP Law 2020 which it can use in furtherance of its objectives. Relevant powers in connection with the enforcement of the DP Law 2020 are set out in the table below.

Ability to audit Controllers and Processors	Article 46(3)(a)
Ability to conduct investigations and inspections	Article 46(3)(b)
Ability to issue directions requiring a Controller or Processor to do or refrain from doing anything (including Processing specified Personal Data)	Article 46(3)(c) and Article 59
Ability to issue warnings or admonishments	Article 46(3)(c)
Ability to make recommendations to a Controller or Processor, including ordering the appointment of a data protection officer	Article 46(3)(c)
Ability to initiate court proceedings for contraventions of the law	Article 46(3)(d)
Ability to impose fines for non-compliance with a direction	Article 46(3)(e) and Article 62[1]
Ability to impose fines for non-compliance with the Law and any Regulations and the ability to set corresponding limits on or schedules of such fines	Article 46(3)(f) and Article 62
Ability to initiate compensation claims on behalf of Data Subjects where there has been a material contravention of the DP Law 2020	Article 46(3)(g)
Ability to prepare Regulations, standards or codes of practice and guidance	Article 46(3)(h) and (i)
Ability to request provision of information from Controllers and Processors	Article 52
Duty to receive and consider complaints lodged by Data Subjects and conduct investigations or meditation between the complainant and the relevant Controller or Processor	Article 60

[1] Fines for certain contraventions are not subject to a maximum limit under Schedule 2 of the DP Law 2020.

Please see the Commissioner's guidance regarding Commissioner's Powers, Fines and Sanctions for further information. You may also wish to check the Commissioner's Individual Rights and Remedies Checklist, available on the Guidance page of the DIFC DP website.

B. Redress regarding unlawful processing of personal data by the public authority: Application of Article 28 to Public Authorities

In addition to the powers set out above, the DP Law 2020 provides a few ways to access redress in specific, legally binding and non-legally binding ways. The following legally binding options provide redress to any individual whose data may have been unlawfully processed by a public authority or law enforcement.

Judicial remedies

Article 63(2) states: "A Data Subject who disagrees with a finding by the Commissioner of contravention of the Law or of no contravention of the Law may appeal against the finding to the Court within thirty (30) days."

Furthermore, a Data Subject who suffers material or non-material damage by reason of any contravention of the DP Law 2020 or the Regulations may apply to the Court for compensation from the Controller or Processor in question. The award of any compensation by the Courts is separate and independent from any fines issued by the Commissioner under the DP Law 2020.

Liability of Controllers and Processors

Articles 64(2) and (3) contain provisions to allocate the risk of compensation between Controllers and Processors. Controllers will always be liable for damage caused by Processing under their control. Where a Processor is involved in the Processing, the Processor will only have liability where it has not complied with the obligations of the DP Law 2020 directed at Processors or where it has acted outside or contrary to the lawful instructions of the Controller (in other words, where it has itself violated the DP Law 2020 or acted outside the proper role of a Processor).

To the extent more than one party is liable for compensation in relation to Processing, Article 64(3) provides for joint and several liability in order to ensure effective compensation of the Data Subject. It will therefore be good practice for Controllers and Processors to clearly address liability issues in their contracts.

Settlement agreements

Parties are free to reach a legally binding settlement of any compensation claim outside court (by mutual agreement).

Commissioner's requests to the Court

Finally, under Article 62(8) the Commissioner may request the Court to make an order for damages or compensation payable to a Data Subject, even if he has not made a claim in accordance with Article 64. The principles in Article 64 will be considered when making the request to the Court. The Commissioner shall not make such requests unless in his opinion the Data Subject in question has suffered material damage as a result of the breach in question and is disadvantaged in his ability to bring a claim to the Court in his own name (for example, due to lack of resource or geographical remoteness or because the facts of the claim are highly complex and may not be available to the Data Subject).

C. Jurisdiction of the DIFC Courts and Enforceability

In accordance with DIFC Court rules and Article 5 of the Judicial Authority Law, Dubai Law No 12 of 2004[2] (the Judicial Authority Law), redress can be exercised where a breach or contravention of the DIFC DP Law 2020 has occurred. A (DIFC) Data Subject may bring a claim against any other party asserting that the DP Law 2020 has been breached, together with the ability to seek damages and compensation. Article 5 of the Judicial Authority Law clarifies that the DIFC Courts have exclusive jurisdiction over DIFC civil and commercial claims. In other words, while a request from a public authority may be based on a criminal investigation, the potential mishandling or unlawful processing of Personal Data outside the scope of such purposes could constitute a contravention of the DIFC DP Law 2020 and is specifically within the exclusive jurisdiction of the DIFC Courts. Further information is set out below to consider after the following case studies.

D. Case Studies

Practical application: If a (UAE or Dubai) public 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 Article 28. All entities in the DIFC have to make an assessment in accordance with this article as outlined above before sharing any Personal Data with such authorities, and all such authorities should recognise the legal basis of the DP Law 2020 given that it ultimately derives from UAE constitutional powers and appointments.

The purpose of the following case studies is to illustrate in a practical manner the redress options that a Data Subject has, where their Personal Data has been unlawfully processed, pursuant to a data transfer request by a public authority. The cases address scenarios where international elements exist, both in respect of the nationality/residency of the Data Subject, as well as of the requesting authority.

[2] https://www.difc.ae/files/7014/5510/4276/Dubai_Law_No._12_of_2004_as_amended_English.pdf

Case study 1

A UK Data Subject is in the UK, for example acting as an ultimate beneficial owner (UBO) or other stakeholder in a DIFC entity. As a result of a request made by a non-DIFC regulator related to a money laundering investigation regarding source of funds, the UK UBO / data subject's information is shared for a specific, regulatory purpose. It is then unlawfully processed by another third party due to intervening circumstances such as accidental loss or breach by the requesting authority, or for otherwise unrelated purposes.

Redress options & Jurisdiction

The remedy options for this UK-based individual seeking redress due to the subsequent unlawful processing (presumably) in contravention of the DP Law 2020, are within the Commissioner's powers to adjudicate, i.e., via a complaint or other remedy under Part 9, and / or the DIFC Courts if raised by the Commissioner.

If an individuals' right to privacy may be compromised by public authorities' interest in obtaining personal data and subsequently unlawfully processing it (or where this is a significant enough risk that this could happen), would, under the DIFC Law and legal / judicial framework, someone (anyone) be able to seek redress?

The answer is yes, and specifically, the jurisdiction would be the DIFC Courts. As set out briefly above, an issue pertinent to DIFC Law is within the jurisdiction of DIFC Courts.

As an example, if DIFC-originating data is requested by a UAE public authority and they do not use it for compatible purposes, such that someone objects and seeks redress, the matter would come to the DIFC courts, as it would be a potential contravention of the DIFC DP Law 2020. In short, the matter comes back to the DIFC for investigation and adjudication.

UBO data requests

Please note, as a brief but important aside, that in relation to UBO data requests, DIFC has employed a detailed process for providing such data and has de-identified it specifically as UBO data. It is in a secure, strictly limited access "vault" that requires two (2) individuals to provide virtual keys to access the information, after approval to do so has been given.

Case study 2

The Personal Data of an individual who is either a customer or a client of a DIFC regulated / DFSA authorised entity, is collected by the DIFC-based Controller and then is shared with onshore UAE authorities for mandatory annual submissions, i.e.: Economic Substance Reports, Common Reporting Standards submissions, amongst others.

In such a case, the processing would again be subject to the requirements of the DIFC DP Law 2020. Ideally, an Article 28(1) conversation would take place and "written assurances" are given, and if not, or in any case, the DIFC entity would have a risk and impact assessment prepared and documented to meet the Article 28(2) elements.

While shared for a regulatory purpose, as with any data sharing, there is no guarantee whether inadvertent data loss or exchange would occur beyond the scope of the specific request's (regulatory) purposes, even with an appropriate risk assessment or with an MOU or other written assurances in place.

The Data Subject may raise the issue to the Commissioner or take any other available recourse provided for in the DP Law 2020 and the DIFC Court Rules. The matter would again come to the DIFC Courts and the process of determining validity of the claim, jurisdiction over the non-DIFC authority and enforcement would again ensue.

Case study 3

Regarding a person who is employed by a DIFC entity within the DIFC. At his request and with understanding of what is needed to be employed with a DIFC entity, his/her Personal Data is collected by the DIFC-based Controller and shared with DIFC Authority and/or various UAE onshore government entities, in order to set up the individual's visa. In short, the data is to be shared in order to receive the required documentation and continue employment.

This case would not likely fall into an Article 28 scenario, owing to the fact that it does not relate to a request by a public authority for data, as envisaged by Article 28.

However, in compliance with the rest of the DP Law 2020, risk assessment and mitigating controls required throughout the DP Law 2020 and in particular under Article 28(2) can and would ideally be in place to ensure that any data shared is handled in accordance with both DIFC's and immigration authorities' statutory obligations. If not, the DP Law 2020 may also be breached in such a scenario and an aggrieved party may seek the previously mentioned redress options.

5. Jurisdiction & Enforceability: Judicial Authority Law, Dubai Law No 12 of 2004

As above, support for the outcomes in these three case studies and any other relevant redress issue again is found in the Judicial Authority Law, Article 5. DIFC Courts have exclusive jurisdiction over matters where there is a nexus with a DIFC Law or authority.

As such, according to DIFC Courts' Enforceability Guidance[3] and protocols, any resulting order could be enforced against any Controller or Processor, including (federal) public authorities. As a reminder, DIFC Courts apply British common law principles and apply British common law case law where warranted.

6. Case Law Updates Regarding Government Access to Personal Data

The Schrems cases are directly related to the importance of Article 28 in the DIFC DP Law 2020 and relevant case studies.

On July 16, 2020**,** the Court of Justice of the European Union in its ruling in the Schrems II case invalidated a data sharing agreement between the EU and the US, called Privacy Shield, as a legitimate transfer mechanism between the US and the EU / EEA. DIFC had not permitted Privacy Shield as a mechanism for international transfers as it applied to transfers and onward transfers from the EU to the US only. In any case, this ruling had a significant impact on data transfers globally and provided a sufficient basis for developing this entirely new article (Article 28) in the DIFC DP Law 2020.

On March 25, 2022, the US Government and the European Commission announced an agreement in principle to a new framework for transfers from the EU to the US, called the Trans-Atlantic Data Privacy Framework (the "Framework"). Please review the White House joint statement with the European Commission setting out the general elements of the framework[4].

DIFC DP Commissioner's Office anticipates that, as above, the Framework will not apply to transfers *directly* from the DIFC as it is an agreement between the EU and the US. However**, if your entity is part of a multi-national or group business that engages in transfers / onward transfers from the EU**, it may come into play. In such cases, please consider reviewing the transfers made by your entity once Personal Data

[3] DIFC Courts Enforcement Guide

[4] The EU Commission joint statement and Fact Sheet are both available as well at the hyperlinks provided.

leaves the DIFC for processing in the EU, to ensure the onward transfers remain compliant with Article 27 of the DIFC DP Law 2020. For further assistance, please review the Data Export assessment tool. Please note that any such guidance is for informational purposes only and should not be construed as legal advice provided by the Commissioner's Office.

7. Conclusion

International data export, sharing and transfers (including onward transfers) – particularly regarding transfers to public authorities and law enforcement as dealt with in Article 28 of the DP Law 2020 - can be quite complex, and will often require professional feedback or legal advice. If you have questions or require clarity on interpretation of Article 28, please feel free to contact the DIFC Commissioner's Office for additional support.

Email: commissioner@dp.difc.ae

Telephone: 04 362 2222

You may also read further general guidance in the DIFC Data Export & Sharing Handbook and by using the Article 28 assessment tool to help you better understand your obligations. Finally, the DIFC Ethical Data Management Risk Index (EDMRI) includes information on sharing data with public authorities and the issues that may cause risk to individuals.