DIFC

# Thematic Assessment Report No. 1 of 2023: Article 28

## Commissioner of Data Protection

# CONTENTS

Introduction ..... 3
Themes Assessed ..... 3
1. Receipt of Government Data Sharing Requests ..... 3
2. Basic Implementation of Article 28 ..... 5
3. Origination of Requests and Processing Operations ..... 6
4. Controller and Processor Obligations, Processing Categories of Personal Data ..... 7
Conclusion and Recommendations ..... 8
5. Conclusion ..... 8
6. Recommendations ..... 8
Appendix 1: Article 28 Government Sharing Thematic Assessment Questions ..... 9

# Introduction

The DIFC Commissioner of Data Protection (the "**Commissioner**") received 178 responses from DFSA-authorized entities or Designated Non-Financial Business or Professions ("**DNFBPs**") to its government data sharing thematic assessment. These responses provide insight into the practical application of Article 28. The questions from the thematic assessment can be found in Appendix 1 of this Report.

Article 28 of the DIFC Data Protection Law sets out the controls and measures for Controllers and Processors to follow upon receiving a request from any public body for the disclosure or transfer of personal data. The Article 28 Thematic Assessment was conducted to help clarify the following concerns for the DIFC Commissioner's Office:

1. Receipt of Government Data Sharing Requests
2. Basic Implementation of Article 28
3. Origination of Requests and Processing Operations
4. Controller and Processor Obligations, Processing Categories of Personal Data

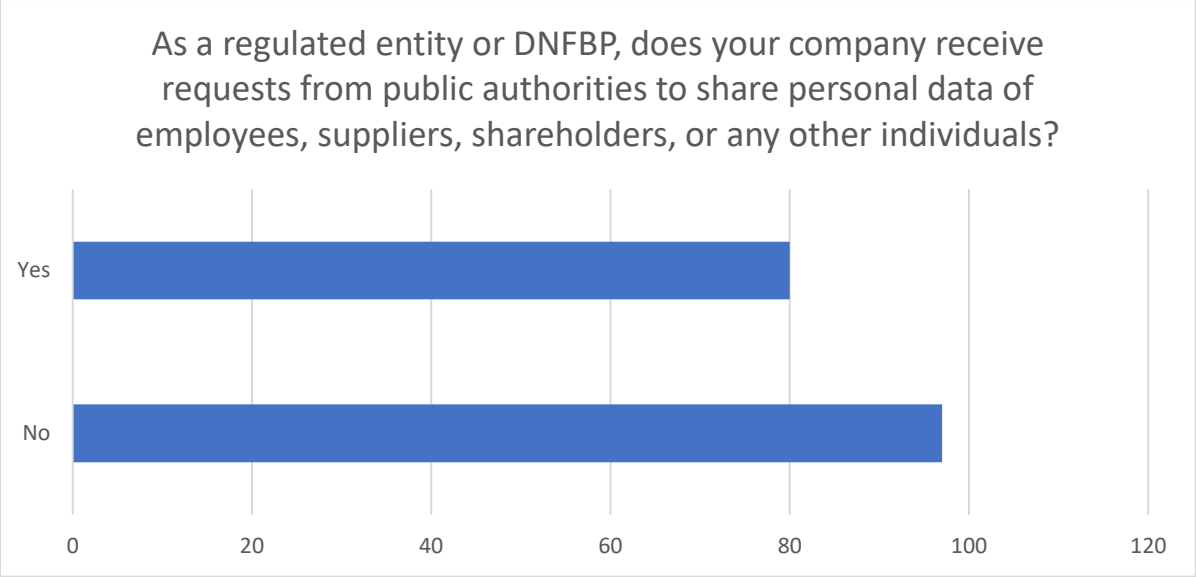
The following Report provides the Commissioner with insight as to where:

- DIFC registered entities that are regulated by the DFSA have appropriately applied Article 28;
- there are gaps that may create risk to the DIFC or its entities; and
- to make improvements in regulations or guidance so that Data Subjects from anywhere in the world whose data is processed in the DIFC are better protected.

# Themes Assessed

1. Receipt of Government Data Sharing Requests

Assessment responses indicate that the majority of regulated DIFC entities or DNFBPs do not receive requests from public authorities to share personal data of employees, suppliers, shareholders or any other individuals. However, approximately 45% responded that they do receive requests. The majority of responses from the assessment did not provide a response to the type of requests received, however, those who did respond confirmed that "regulatory requirements *other than* financial crime investigations" were often requested. The limited number of respondents that selected "Other" as a response to the types of requests received, mainly indicated that these are administrative in nature.




To briefly clarify, Article 28 covers requests made internally (within the DIFC) as well as externally (outside the DIFC). In this regard, for example, some responses explained that the types of government requests could include requests for employee visa purposes or to fulfil DIFC or DFSA regulatory and compliance requirements.

Lack of awareness and understanding about the type of data sharing requests companies could receive from public bodies, as well as the scope of Article 28, could explain the results received.

The numbers regarding requests received from DIFC authorities (e.g., DIFCA and DFSA) does not diminish the applicability of Article 28, which applies to requests from "…*any* public authority over the person or any part of its Group." However, in the case of employment visa request, for example, the Data Subject is normally directly involved and has provided consent for a known, specific purpose whereas for DFSA regulatory requests, consent or knowledge of the transfer (even within the DIFC) may not even be communicated to the Data Subject due to an investigation or other purposes within the DFSA's regulatory remit. For the latter, additional consideration according to Article 28 should be taken.

Considering the regulatory landscape of the UAE and applicability or objectives of certain onshore laws, Article 28 in large part aims to levy additional measures on DIFC-based entities responding to public authority requests from *outside* the DIFC. These could include requests from law enforcement authorities, UAE Central Bank, UAE Financial Intelligence Unit or Federal Tax Authority. As the assessment questions indicate, other purposes of requests could be for financial crime reporting or investigations, or court orders.

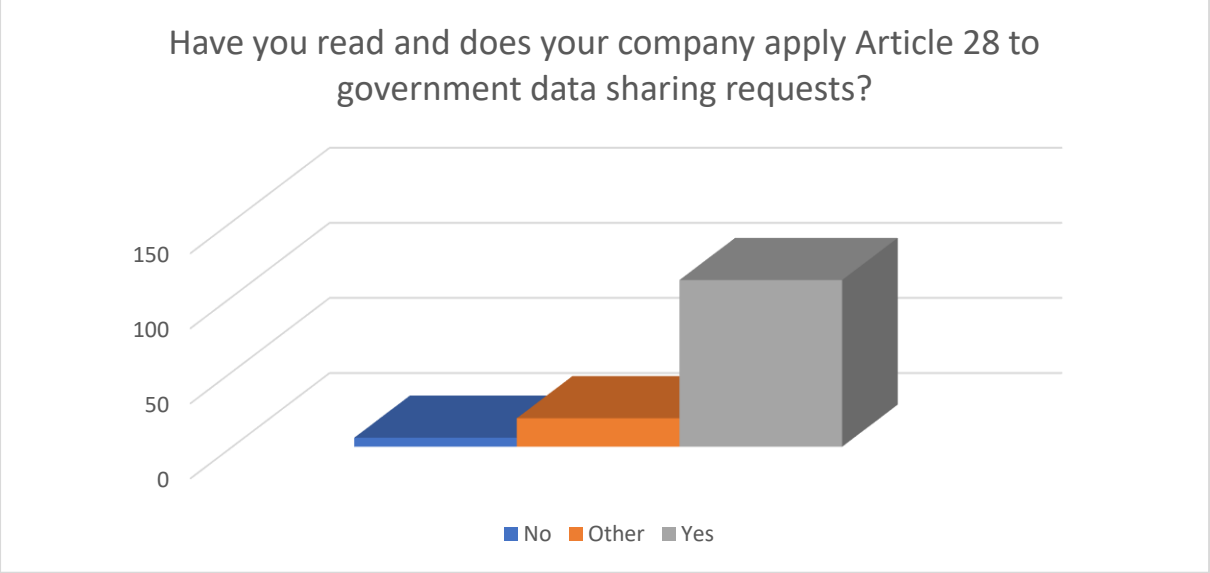
To be sure, although the focus in the above example was on UAE government authority requests as a consequence of factors such as proximity and local inter-jurisdictional regulatory obligations, the same measures must be applied regardless of where the Requesting Authority is located. In principle, whether the request comes from the United Kingdom, Brazil, China, the United States or anywhere else in the world, the Controller has the primary responsibility of applying such measures and ensuring the transfer is safeguarded from the outset. Accordingly, in the absence and regardless of redress mechanisms or other circumstances in the requesting jurisdiction that may impact the rights of a Data Subject, the Commissioner

may exercise his powers to apply to or initiate proceedings for contraventions of the DP Law before the DIFC Courts, as set out in Article 46(3)(e) and Article 59(5), and any other relevant provisions in the DP Law or DP Regulations.

Therefore, through this assessment theme, certain nuances between types of government data sharing requests ought to be clarified and further guidance or case studies provided to better understand the use and application of Article 28. Doing so will not only increase effective implementation of Article 28, but will better serve the Data Subjects whose data is being shared with both internal and external authorities.

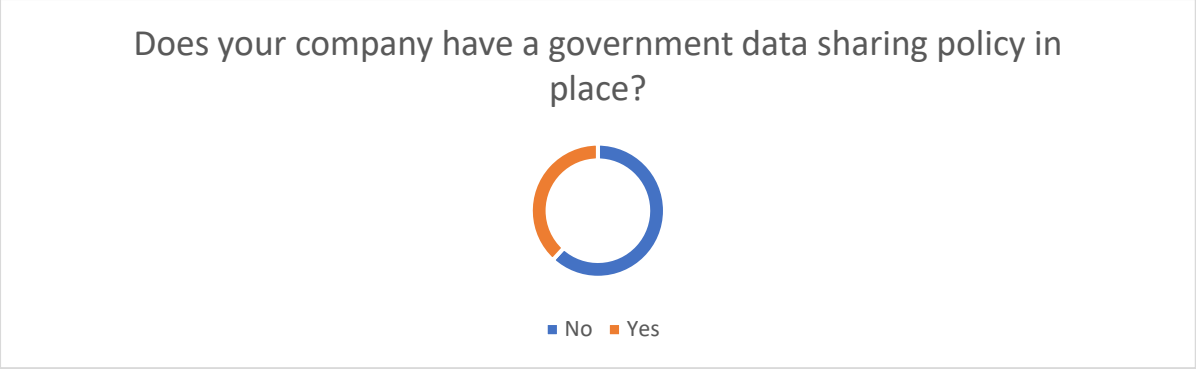
## 2. Basic Implementation of Article 28

Over 60% of DIFC entities or DNFBPs read and apply Article 28 to government data sharing requests. Nonetheless, it is required that all entities familiarise themselves with Article 28 and to set up the relevant processes in the event a request is received.



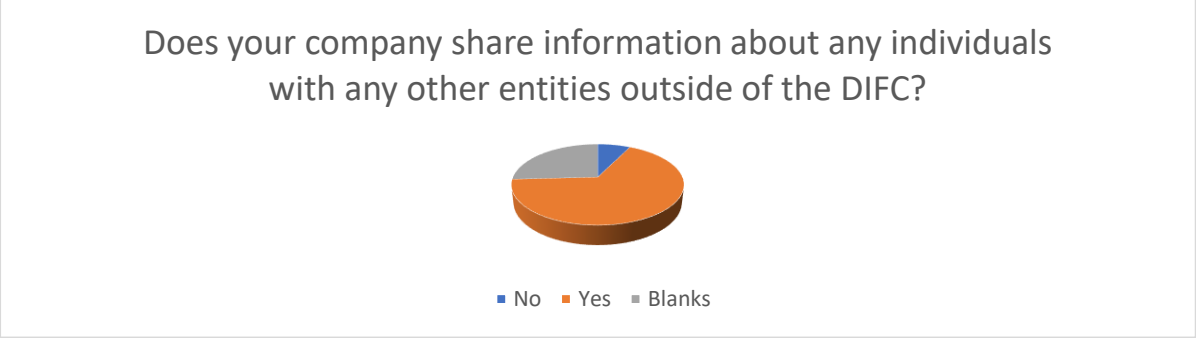

The assessment also revealed that over 60% of regulated entities or DNFBPs do not have a government data sharing policy in place. Although some responses show that most entities adopt Standard Contractual Clauses (DIFC or others) or rely on adequacy decisions for the transfer of personal data outside the DIFC, entities are generally reminded to follow Articles 26 and 27 closely and comply with requirements to safeguard data transfers.[1] In particular, since the UAE is currently not listed as an adequate jurisdiction, sending data to public authorities in the UAE in response to a request should be in accordance with Article 27 (as well as Article 28).

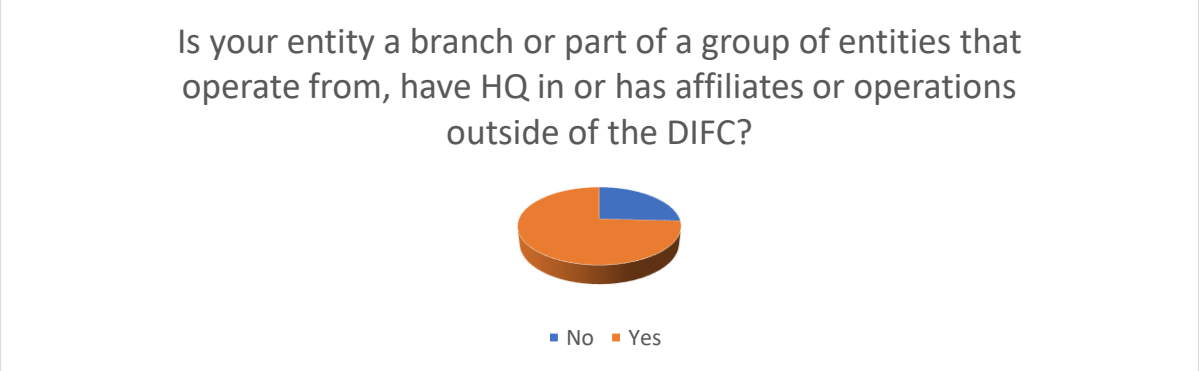
[1] Please refer to the DIFC Export and Sharing Handbook for more information: https://www.difc.ae/business/operating/data-protection/guidance/#s17




3. Origination of Requests and Processing Operations

The assessment showed that nearly 75% of entities who responded, are a branch or part of a group of entities that operate from, have HQs in or have affiliates or operations outside of the DIFC and most entities share information about individuals with the other entities (outside the DIFC). Entities are reminded that even for intra-group transfers, Articles 26 and 27 of the DIFC Data Protection Law need to be followed.



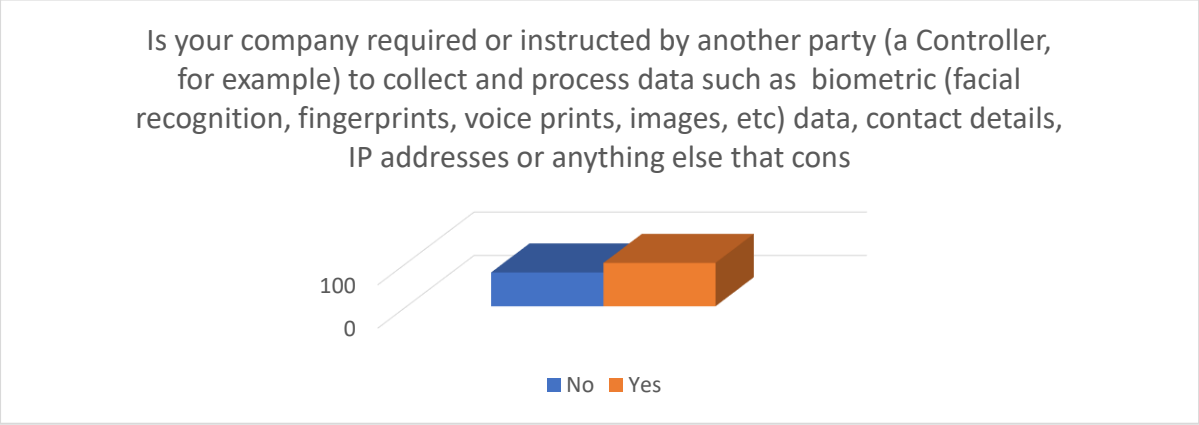




Additionally, while most respondents did not specifically explain the type of public authorities that government requests come from, certain responses indicated that most requests come from local and regional authorities either in the UAE or GCC. Others indicated that requests are received from international law enforcement and authorities. One response indicated that

this includes requests from authorities based where company headquarters or majority of operations are. This will likely be the case for other entities receiving international requests including from, for example, the US government (under the FATCA requirements, Securities and Exchange Commission, etc) or UK bodies. The Commissioner expects DIFC entities to implement the same level of due diligence and controls to international as well as local requests.

4. Controller and Processor Obligations, Processing Categories of Personal Data

The assessment also provided insight into whether the entity is required or instructed by another party (a Controller, for example) to collect and process data such as biometric (facial recognition, fingerprints, voice prints, images, etc) data, contact details, IP addresses, or anything else that constitutes personal information. The majority of entities answered “Yes”. In those instances, additional obligations in relation to Special Categories of Personal Data (such as Article 11) need to be satisfied.



# Conclusion and Recommendations

## 5. Conclusion

The Article 28 assessment demonstrates that awareness of the DIFC DP Law is growing amongst companies based in the DIFC. However, specific requirements beyond the general principles and basic processing obligations are not fully understood or applied.

Article 28 is key to ensuring data flows with trust to government authorities and that it is managed with trust by government authorities. A good example of this is an advisory letter shared with the US Securities and Exchange Commission for proper data sharing with DIFC regulated entities. In addition to reading the black letter Articles, practical applicability of the tenets of Article 28 are set out clearly regarding assurances that data will be managed with good governance structures but also that it will not act as a barrier to open data sharing for substantial public interests, as needed.

Even so, out of the limited number of respondents that provided details to the types of government authority and law enforcement requests query, the requests received include internal requests within the DIFC, including DFSA and DIFC Courts. We assume this would be consistent with other potential respondents, and may enquire further via inspections or an addition assessment (see recommendations below). The primary purposes of these requests are to provide information for visa applications, employment administration, financial services reporting, risk assessments and similar activities that the individual Data Subject is commonly directly participating in at their request or for company compliance with applicable laws (FATCA, Economic Substance, Common Reporting Standard all being examples). DIFC businesses do receive requests from government authorities based both locally and abroad, but less risk is presented in such cases as they are often complying with regulatory reporting requirements by way of answering follow up queries and providing further evidence of compliance, and in such cases the information shared may not likely be personal data. In some cases, they could be responding to flow down requests from their corporate headquarters or within the group of companies.

## 6. Recommendations

As a follow up to the Article 28 Thematic Assessment, the Commissioner's Office will aim to provide additional outreach and information sharing sessions about the Article and its requirements, engage in round table discussions, and promote the available guidance and assessment tool regarding Article 28.

The automated inspection module will also be updated to specifically capture feedback and analytics about Article 28 in practice for all DIFC entities, as the thematic review in this instance was limited to regulated entities and DNFBPs.

A further review will be conducted within two (2) years to measure improvement and implementation of Article 28.

# Appendix 1: Article 28 Government Sharing Thematic Assessment Questions

1. Have you notified that your business does or does not process Personal Data?

   Response options:

   - Yes, processes
   - No, doesn't process

   *Sub Question*:

   If no, please provide reasons that you notified that your business does not process personal data

2. How did you determine what Personal Data is and whether your business processes (i.e., stores, shares, etc) it?

   Response options:

   - We have / don't have employees
   - We have / don't have clients or customers
   - We engage / don't engage with suppliers or other third parties
   - We collect / don't collect personal data from other sources

3. Do you have business contact information of any clients, employees or suppliers, including biometric information, that you store in email accounts, CRM, or cloud or physical servers?

   Response options:

   - Yes
   - No

4. As a regulated entity or DNFBP, do you receive requests from public authorities (i.e., Requesting Authorities as defined in Article 28 of the DIFC DP Law 2020) to share personal data of employees, suppliers, shareholders, or any other individuals?

   Response options:

   - Yes
   - No

   *Sub Question*:

   Please provide details about the requests received

Response options:

- Financial crime reporting / investigations
- Court Orders
- General welfare and individual satisfaction
- Regulatory requirements other than Financial crime investigations
- All of the above
- Other

4.1 What types of public authorities do the requests come from?

Response options:

- International authorities
- Local / Regional authorities
- Local / Regional law enforcement
- International law enforcement
- All of the above
- Other

5. What kind of technical, organisational, or security measures or policies do you have in place to ensure the security of the systems used to process personal data?

*Sub-Question 1:*

Have you read and do you apply Article 28 to government data sharing requests?

Response options:

- Yes
- No
- Other

5.1 Do you have a government data sharing policy in place?

Response options:

- Yes
- No

*Sub Question 1*:

Do you apply any of the following appropriate safeguards to data export from the DIFC in accordance with Articles 26 or 27 of the DP Law 2020?

Response options:

- Yes
- No

*Sub-Question 2*:

Do you regularly conduct data protection impact assessments?

Response options:

- Yes
- No

6. To provide your services to clients or employees, are you required or instructed by another party (a Controller, for example) to collect and process data such as biometric (facial recognition, fingerprints, voice prints, images, etc) data, contact details, IP addresses, or anything else that constitutes personal information?

   Response options:

   - Yes
   - No

7. Is your entity a branch or part of a group of entities that operate from, have HQ in or has affiliates or operations outside of the DIFC?

   Response options:

   - Yes
   - No

*Sub-Question:*

Do you share information about any individuals with the any other entities outside of the DIFC?

Response options:

- Yes
- No