ARTICLE 28

FAQs

Where can I find more information on the process of responding to requests from public authorities?

Article 28 of DIFC Data Protection Law 2020 prescribes the process a DIFC entity ought to follow in handling and responding to such requests. For a detailed overview of the process please refer to the Commissioner's guidance on Article 28. Additionally, in case the requesting public authority is outside the jurisdiction of the DIFC, also consult the Data Export and Sharing Handbook with respect to applying the Article 26 and 27 safeguards when transferring data outside of the DIFC.

Why did DIFC introduce Article 28 to DIFC Data Protection Law 2020?

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.

How does our company comply with Article 28 when responding to data requests from public authorities?

Article 28 provides the DIFC 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 (2) phases:

i. Phase 1, under Article 28(1), which provides for the initial assessments you ought to engage in with the Requesting Authority, where possible, 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.

Refer to the Commissioner's guidance on Article 28 for a detailed overview of the two phases and of the individual steps within each phase. You may also wish to try the Article 28 Assessment Tool, which will give you more specific guidance about next steps to take and what other considerations, including Article 26 and 27 requirements, to complete the Article 28 compliance package.

When transferring data to a public authority that is outside of the DIFC's jurisdiction, other than Article 28 safeguards, what other requirements apply?

Further to the Article 28 process, in case the requesting public authority is not a DIFC body (DIFC Authority, DFSA or DIFC Courts) and the data – if you are to respond positively to the request – is subsequently transferred outside of the DIFC, either to the UAE mainland or to any other jurisdiction globally, you must also apply the safeguards prescribed by Articles 26 and 27 of DIFC Data Protection Law 2020. For more information please refer to the Data Export and Sharing Handbook.

More specifically, where Personal Data is leaving the DIFC to a jurisdiction:

i. that is not deemed by the Commissioner to have an equivalent data protection law to that of DIFC DP Law 2020 in accordance with Article 26; or

ii. where certain risks in relation to the importing entity are higher than usual, as set out in the Ethical Data Management Risk Index (EDMRI) and as identified by an assessment of the importing entity as per the EDMRI+ tool,

the DIFC exporting entity will be required to apply additional safeguards, such as the DIFC Standard Contractual Clauses or conducting additional due diligence to mitigate the risk and document its decision-making, or both. All supporting information for these obligations are outlined on the Data Export & Sharing sub-menu of the DIFC DP website.

How can the validity and proportionality of the request be determined?

When a DIFC entity receives a request from a public authority, one of the first steps is to determine the validity and proportionality of such request.

In that respect, the DIFC entity needs to exercise reasonable caution and due diligence 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.

Regarding proportionality, 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, the DIFC entity should validate the purpose and limit the scope in order to minimize the sharing and specify the reason for the processing.

What should be analysed in an Impact Assessment and what measures could be taken to minimise these risks?

The risk assessment will focus on assessing the impact of the proposed transfer in light of the potential risks to the rights of the affected Data Subjects, i.e., 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.

Further to the above, to ensure proper due diligence, you should include in your consideration the following when assessing the risks of 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.

Following the completion of this assessment, you ought 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.

What are the "written assurances" in Article 28(1)(c) and what if I cannot obtain such from the requesting public authority?

When processing the 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.

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

i. a basic data sharing Memorandum of Understanding (MOU);

ii. an annex to the DIFC Standard Contractual Clauses (SCCs);

iii. a simple email agreement citing Article 28 of the DP Law 2020; or

iv. a full data protection agreement.

The DIFC DP Accountability & Rights website has an Article 28 MOU template that you may wish to use for these purposes. The DIFC Commissioner's Office is available to consult on possible forms of "written assurances" and whether pursuit of obtaining this safeguard is warranted.

The Commissioner's Office recognizes that in some instances (i.e., court orders or other similar evidentiary demands) obtaining written assurances under Article 28(1)(c) is not always possible, so while important, this element is not determinative of compliance with Article 28.

What are the available redress remedies for a Data Subject in case of an Article 28 breach?

DIFC Data Protection Law 2020 provides multiple ways to access redress in specific, legally binding and non-legally binding manners to any individual whose data may have been unlawfully processed by a public authority or law enforcement.

From a high-level perspective, such remedies are categorized as follows:

i. remedies pursuant to the Commissioner's authority, as the Commissioner has a range of powers available to monitor, ensure and enforce compliance with the law; and

ii. judicial remedies, as a Data Subject may bring a claim for compensation to the DIFC Courts against any other party asserting that the DP Law 2020 has been breached.

Please see section 4 of the Commissioner's Article 28 guidance for a detailed overview of the available redress remedies. For further information refer to the Commissioner's guidance regarding Commissioner's Powers, Fines and Sanctions. You may also wish to check the Commissioner's Individual Rights and Remedies Checklist, available on the Guidance page of the DIFC DP website.

Do the DIFC Courts have jurisdiction in cases where Data Subjects are non-UAE nationals or residents and where the Requesting Authority is not a DIFC Body?

The remedy options for a non-UAE national and/or non-UAE resident seeking redress due to the subsequent unlawful processing (presumably) in contravention of the DIFC Data Protection Law 2020, are within the Commissioner's powers to adjudicate, i.e., via a complaint or other remedy under Part 9 of the law, as well as within the jurisdiction of the DIFC Courts.

More specifically, as per Article 5 of the Judicial Authority Law, Dubai Law No 12 of 2004, the DIFC Courts have exclusive jurisdiction over DIFC civil and commercial claims, including claims pursuant to contraventions of DP Law 2020.

As such, according to DIFC Courts' Enforceability Guidance and protocols, any resulting order could be enforced against any Controller or Processor, including (federal) public authorities. With respect to enforcement of judgments outside the UAE, refer to section 3 of the above guidance.

Can I consult with the DIFC Commissioner's Office if I need more help?

Article 28(3) of DIFC Data Protection Law 2020 provides for the option of consulting with the Commissioner's Office in relation to a data request by a public authority. Hence, it is possible for both the DIFC entity and / or the requesting government authority to receive guidance from the Commissioner's Office.