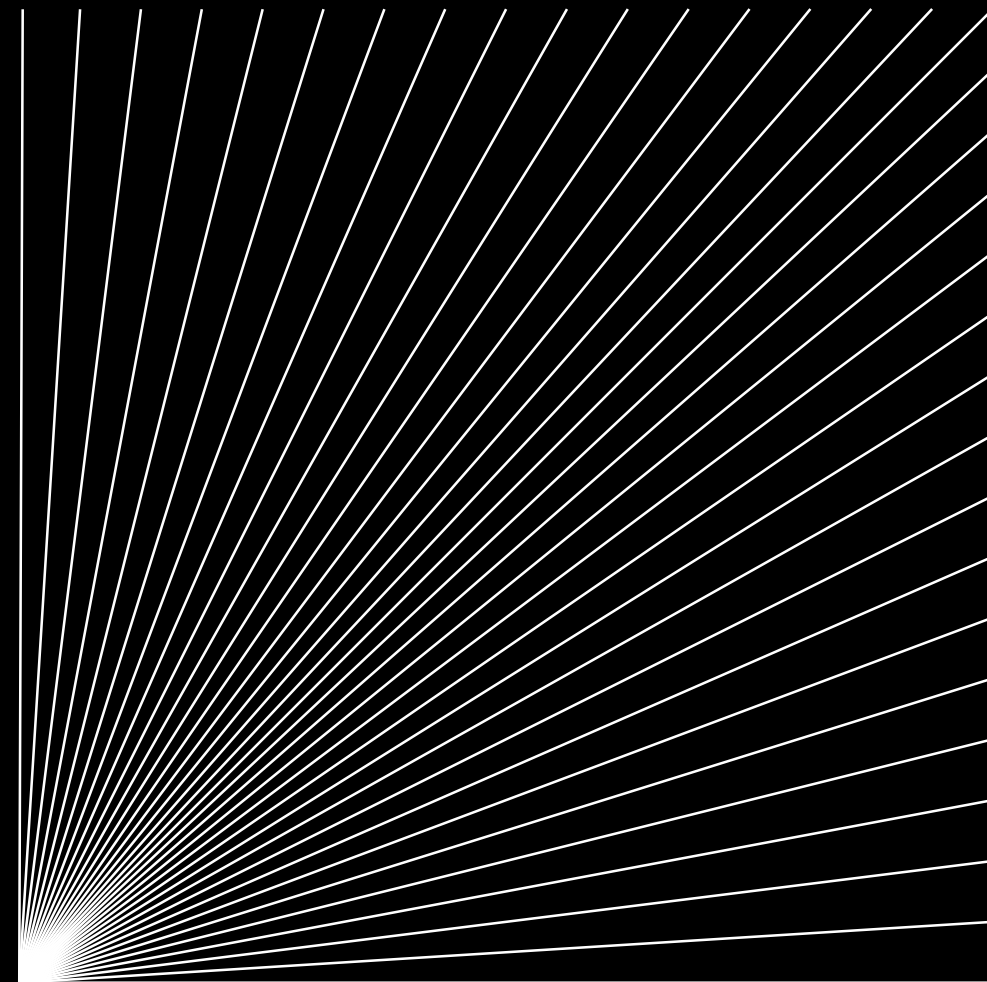


# DIFC Data Protection Talks

Talk #6: Article 28

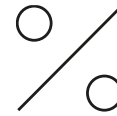
Date: 4 October 2022

**The future is here.**

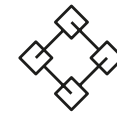




**What is Article 28 about?**



**How do I implement Article 28?**



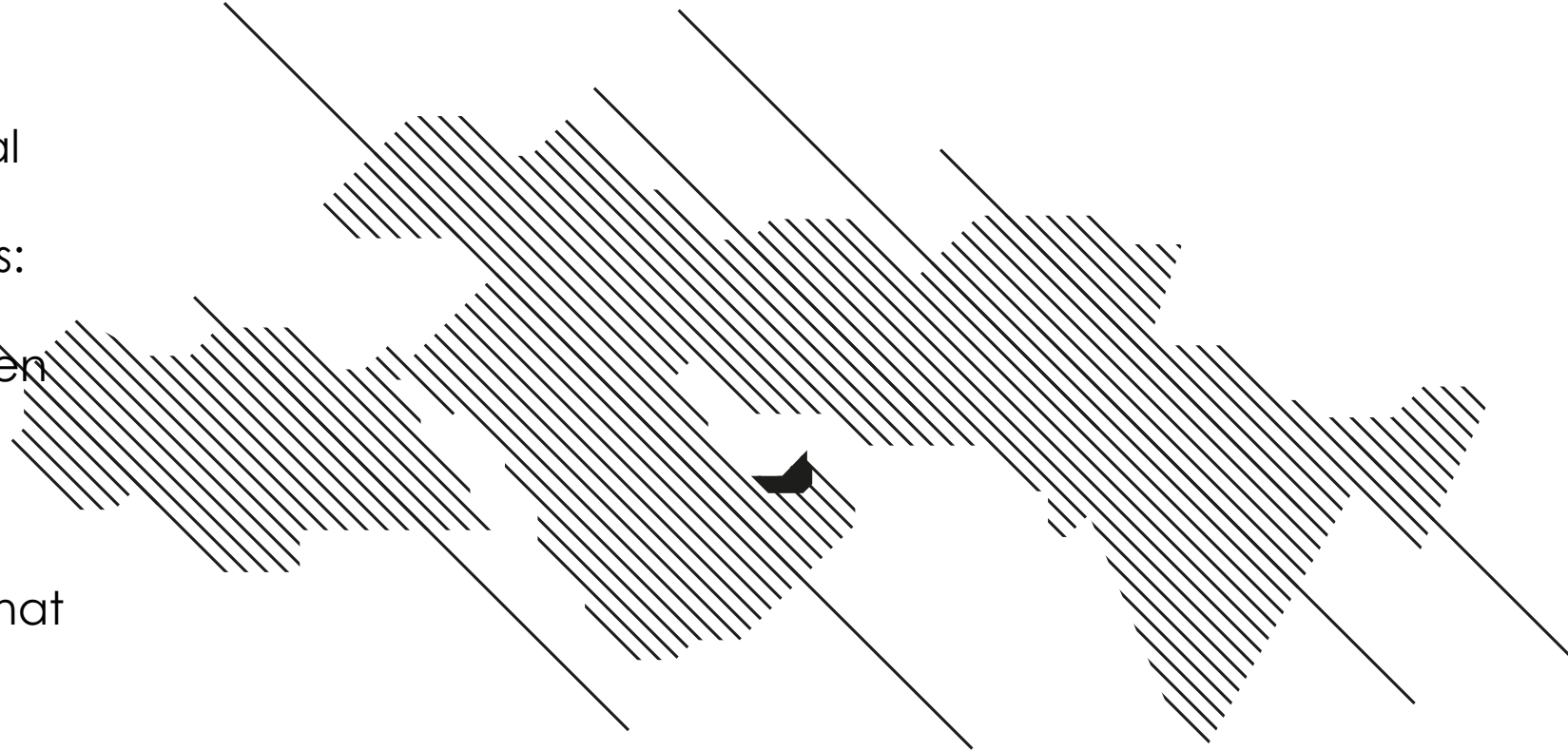
**What are your burning questions?**

# What is Article 28 about?

---

DIFC DP Law 2020 introduced an article to address the important accountability measures to implement when sharing personal data at the request of a government authority. It includes:

- a) Requirement to obtain “written assurances” where possible; and
- b) Conducting a DPIA or other measures to assure yourself that the importer is safe and compliant



## Article 28

[Directive 4 of 2022](#) issued September 2022

## 1

[Assessment tool](#) to assist your understanding of how to implement A28

## Guidance

Article 28 FAQs and guidance are available [here](#)

# How do I implement Article 28?

Article 28 **IS NOT** meant to...

1. Stop you sharing personal data with a government authority or law enforcement.
2. Be used to unnecessarily prolong or obstruct the exchange of information process
3. Be read alone or out of context

Article 28 **IS** meant to...

1. Help you make decisions about the safety of personal data when shared with a non-DIFC authority
2. Ensure that the non-DIFC authority understands the safeguards and principles in the DIFC DP Law 2020 and – hopefully – applies them.
3. Assure the rights of data subjects regardless of what the request for personal data is about.



# What else do I need to know about Article 28?

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



As a data subject, can I raise a concern about a government authority or law enforcement if my PD is unlawfully processed?



Do Articles 26 and 27 apply if I transfer PD outside of the DIFC even to a public authority?



Does the DIFC Courts enforce my rights as a data subject?



Under which specific circumstances may a non-DIFC public authority lawfully access data held within DIFC?



What remedies to I have as an individual if my data was unlawfully processed?



What are “written assurances”?



Can I consult with the Commissioner’s Office if I need help understanding A28?

# What are YOUR burning questions?

<b>How can we handle multiple data access or data share requests from government and its entities?</b>	Article 28 provides obligations that controllers and processors must consider when sharing personal data with any government authorities or law enforcement, not only mainland authorities. If you are required by court order or similar to share data, you may not have a choice to implement A28, but the general idea is to apply the DP principles in DP Law 2020 as much as possible to such requests, even where there is a conflict of laws. Guidance will be provided on A28 specifically by the end of July, and the <a href="#">Data Export &amp; Sharing Handbook</a> will also be updated accordingly.
<b>Please provide a quick review on personal data and sensitive personal data and are the definitions in line with EU/UK Data Protection regulations.</b>	DP Law 2020 Schedule 1, Article 3 sets out all definitions, for general reference. Both definitions are effectively the same as the GDPR and UK GPDR. Personal Data is anything that identifies an individual, and sensitive data (aka Special Category data) is that which has a subjective quality to it such as race, health, sexuality, biometrics, etc. Same as GDPR.
<b>Please discuss rights of the data subjects, cross border data transfer, data breaches and notifications</b>	Please review the General Guide to DP Law 2020, as well as specific <a href="#">guidance</a> per topic. Generally, all topics are aligned with best practice and international DP law principles. Subject access and erasure, control, etc., must be provided for. Cross border transfers outside of DIFC will depend on a risk assessment and equivalence of laws, as well as environment. Breaches must be notified if there is a risk that DS rights are compromised. Notifications are required when processing Personal Data.
<b>Standard Contractual Clauses templates - are these available? What do we need to look at in particular, when doing this?</b>	<p>DIFC has developed Standard Contractual Clauses (SCCs). Please have a look <a href="#">here</a> for the DIFC SCCs template. The DIFC SCCs template is modeled after on the equivalent UK / GDPR templates.</p> <p>The Data Export &amp; Sharing Handbook provides practical application tips with respect to the SCCs, i.e., on the occasion that you are required to use EU Model Clauses. As a note, SCCs are one safeguard measure amongst many. DIFC has issued the <a href="#">Ethical Data Management Risk Index</a> and the EDMRI+ (EDMRI and EDRMI+) tool, which will assist DIFC exporting entities to understand potential risks of the importing entity breaching relevant data protection laws.</p> <p>The most common issue we get asked about is regarding international transfers of personal data and what to do to ensure compliance with the many different laws on this. The EU is on one end of the spectrum for specific, technical requirements, whereas other regulators have their own degrees of requirements. DIFC's requirements are set out in our Data Export &amp; Sharing Handbook. Please have a look at the <a href="#">Data Export &amp; Sharing link</a> of the DIFC website for more support.</p>

Tru  
Trust  
Share

## Contact

---

For further information  
please contact:

DIFC DP Commissioner's Office  
[commissioner@dp.difc.ae](mailto:commissioner@dp.difc.ae)

+971 4 362 2222

Gate Building  
Level 14  
DIFC, Dubai, UAE  
PO Box 74777