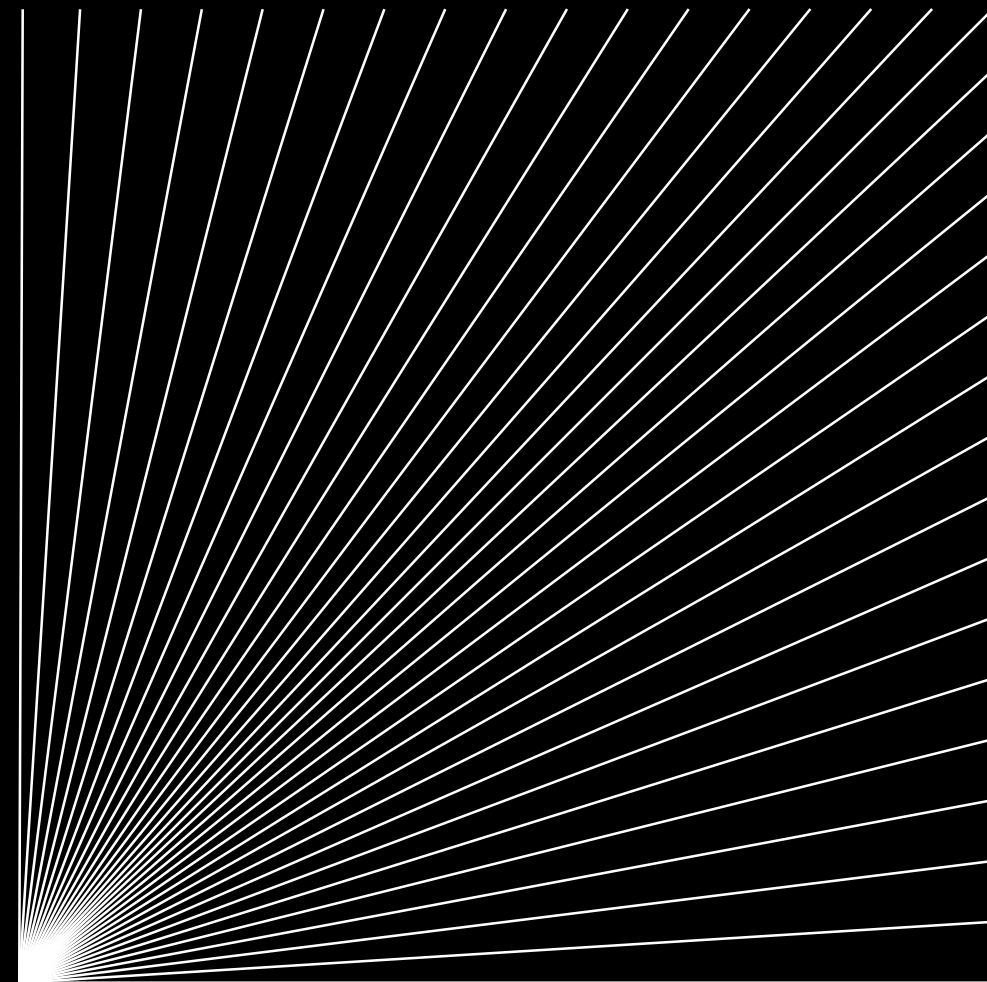


DIFC Data Protection Talks

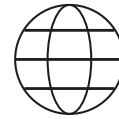
Talk #5: DPO Annual Assessment

Date: 19 July 2022

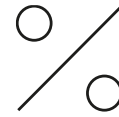
The future is here.



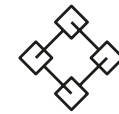
Discussion



What is the DPO Annual Assessment and do I have to complete it?



How long does the DPO AA take to complete and what are next steps when it's submitted?

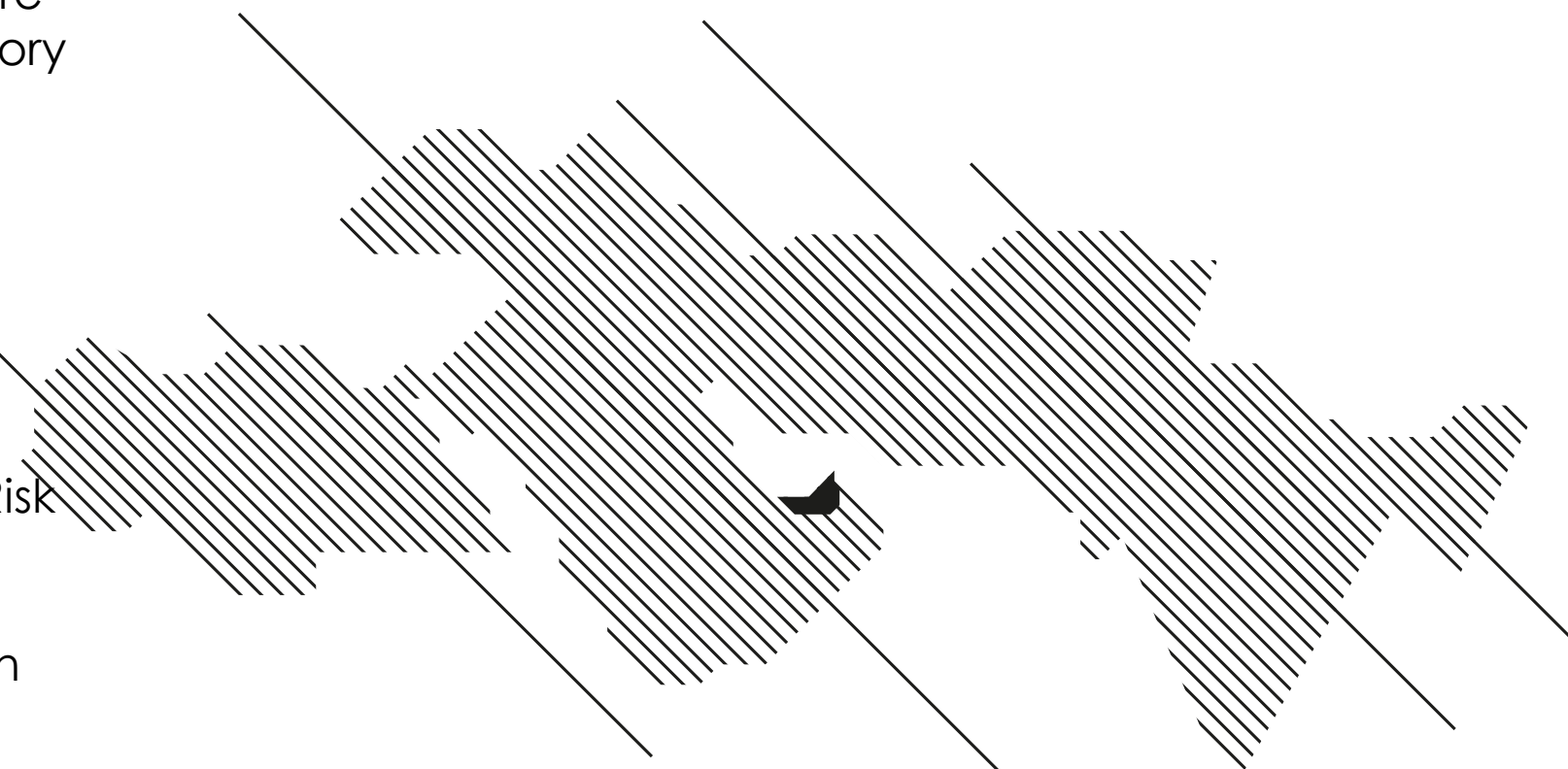


What are your burning questions?

What is the DPO Annual Assessment and do I have to complete it?

Data protection officers (DPO) are an important part of any regulatory compliance program as an accountability champion for the company he or she represents:

- a) meant to be independent;
- b) DPO is not a mandatory appointment, only for High Risk Processing; and
- c) DPO must annually submit an assessment of the entity's processing activities.



Article 19

Since July 1, 2021, DPOs have been required to comply with this article

53

Annual Assessments have been submitted in 2022

Guidance

DPO appointment and obligations guidance is available [here](#)

How long does the DPO AA take and what are the next steps?

1. The DPO Annual Assessment takes about 45 minutes maximum to complete.
2. It is auto-approved in the client portal, and then a sampling are reviewed on a regular basis.
3. It is not mandatory to upload documents, but there is an option to do so if that is helpful to explain the processing activities.
4. As part of the process, you are given a risk matrix, developed by the Commissioner's Office, that will help you understand the types of risks that your company's processing creates, and the rationale for mitigating them.
5. Sample DPO Assessment template:
<https://www.difc.ae/business/operating/data-protection/accountability/#s4>



What does the DPO Annual Assessment cover?

What if I know my company is not compliant with the DP Law 2020 when being inspected?



What if I don't respond to an inspection request?



What activities does my business perform?



How many Processors are we sharing data with and what DP laws are in place where they operate?



Where does my company collect Personal Data?



Can I request an extension to respond to an inspection request?



Does any data leave the DIFC?



Have I evaluated the risk that processing creates regarding the personal data we store?

What are YOUR burning questions?

<p>How can we handle multiple data access or data share requests from government and its entities?</p>	<p>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 Data Export & Sharing Handbook will also be updated accordingly.</p>
<p>Please provide a quick review on personal data and sensitive personal data and are the definitions in line with EU/UK Data Protection regulations.</p>	<p>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.</p>
<p>Please discuss rights of the data subjects, cross border data transfer, data breaches and notifications</p>	<p>Please review the General Guide to DP Law 2020, as well as specific guidance 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.</p>
<p>Standard Contractual Clauses templates - are these available? What do we need to look at in particular, when doing this?</p>	<p>DIFC has developed Standard Contractual Clauses (SCCs). Please have a look here for the DIFC SCCs template. The DIFC SCCs template is modeled after on the equivalent UK / GDPR templates.</p> <p>The Data Export & 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. By the end of Q3, DIFC will also release the Ethical Data Management Index+ (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 & Sharing Handbook. Please have a look at the Data Export & Sharing link of the DIFC website for more support.</p>

What are YOUR burning questions? (/2)

<p>What are the contractual obligations of controllers and processors under DP Law 2020?</p>	<p>Articles 23 to 25 of DP Law 2020 provide for the respective responsibilities of controllers and processors. Additionally, these Articles prescribe the legal relationship arising between the two, as well as the written agreements they can enter into. New guidance is available on the DIFC website with respect to their agreements and obligations.</p>
<p>What is the retention period for personal data of data subjects (in years)?</p>	<p>There is no specified period under the DP Law 2020. The retention of personal data will depend on multiple factors, such as the processing (i.e., when the basis for processing changes under Article 22), exercise of data subjects' rights (i.e., right to withdraw consent under Article 32) and other legal requirements. Retention guidance is available here.</p>
<p>Who is responsible for enforcing the DP Law 2020?</p>	<p>The DIFC Commissioner of Data Protection and the DIFC Courts, when required, deal with the enforcement of the DP Law.</p> <p>The Commissioner has a wide range of powers available under DP Law 2020, i.e., conducting investigations, imposing fines, issuing directions, receiving complaints lodged by data subjects and initiating court proceedings for contraventions of the law, amongst others. Additionally, the DIFC Courts have jurisdiction over claims arising in cases where the DP Law 2020 is applicable. Relevant guidance is available here.</p> <p>With respect to mainland UAE, the regulator charged with overseeing the new UAE DP Law is the UAE Data Office. Complaints can be filed with the UAE Data Office by any data subject. However, please note that the UAE Data Office has not commenced operations yet. The UAE DP Law does not specify whether data subjects can bring a claim before a competent court for compensation.</p>
<p>An employee of DIFC company publishes on LinkedIn description of his conflict with GM of a company. What are the consequences?</p>	<p>The answer to this question would depend on the individual facts of each case, as different provisions would apply depending on whether personal data are included in such post.</p> <p>To begin with, you should first consider whether the information contained in the post breaches any company privacy policies and any NDA or Employee (confidentiality) contracts or agreements. Further, general provisions of civil law could be applicable.</p> <p>With respect to data protection contraventions, revealing personal information about the “GM”, including in connection with his company role (even if such information could be publicly available elsewhere), could breach privacy principles and compromise the company’s compliance with data protection laws.</p>

Tru
Trust
Share

Contact

For further information
please contact:

DIFC DP Commissioner's Office
commissioner@dp.difc.ae

+971 4 362 2222

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